АЛГЕБРА 1

ЗОРАН ПЕТРОВИЋ

Предавања за школску 2014/15 годину

Групе

Основни појмови и примери

Групе су један од централних објеката у овом курсу и неколико недеља ће бити посвећено управо њима. Појам групе може се увести на два еквивалентна начина.

Дефиниција 1 Група је алгебарска структура $(G, \cdot)$, где је G непразан скуп, а $\cdot$ бинарна операција на скупу G, за које важи:

1. за све $x, y, z \in G$: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
2. постоји $e \in G$ тако да је за сваки $x \in G$ испуњено: $x \cdot e = x = e \cdot x$;
3. за сваки $x \in G$ постоји $\bar{x} \in G$ тако да је $x \cdot \bar{x} = e = \bar{x} \cdot x$.

Дефиниција 2 Група је алгебарска структура $(G, \cdot, ', 1)$, где је G непразан скуп, $\cdot$ бинарна операција на скупу G, $'$ унарна операција на скупу G и 1 изабрани елемент из G, за које важи:

1. за све $x, y, z \in G$: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
2. за све $x \in G$: $x \cdot 1 = x = 1 \cdot x$;
3. за све $x \in G$: $x \cdot x' = 1 = x' \cdot x$.

Покажимо да су ове дефиниције еквивалентне.

Ако је $(G, \cdot, ', 1)$ група у смислу друге дефиниције онда је тражени елемент e из прве дефиниције заправо 1, док је за $x \in G$ тражени елемент $\bar{x}$ заправо x'. Дакле, то је доста једноставно. Нешто је теже показати како се на основу структуре из прве дефиниције добија структура из друге.

Претпоставимо да је структура $(G, \cdot)$ група у смислу прве дефиниције. Приметимо да је елемент e (који се зове неутрал групе), из ове дефиниције, јединствено одређен. Наиме, претпоставимо да постоји и елемент f који задовољава исте услове као и e. Тада добијамо да је $e \cdot f = f$ пошто је e неутрал, али је и $e \cdot f = e$ пошто је f неутрал. Дакле, $e = f$. За изабрани елемент, који нам треба у другој дефиницији узимамо елемент e.

Да бисмо имали дефинисану унарну операцију $'$ на скупу G, која задовољава услове из друге дефиниције, покажимо да је за дати елемент $x \in G$ елемент $\bar{x}$ (који се зове инверз елемента x) јединствено одређен. То се показује на сличан начин као и јединственост неутрала. Претпоставимо да, осим $\bar{x}$, постоји и елемент $\tilde{x}$, који задовољава исте

услове. Тада је $\tilde{x} \cdot (x \cdot \bar{x}) = \tilde{x} \cdot e = \tilde{x}$, но такође је $\tilde{x} \cdot (x \cdot \bar{x}) = (\tilde{x} \cdot x) \cdot \bar{x} = e \cdot \bar{x} = \bar{x}$ и добијамо да је $\tilde{x} = \bar{x}$. Дакле са: $x' := \bar{x}$, при чему је $\bar{x}$ јединствени елемент из прве дефиниције, добијамо добро дефинисану унарну операцију, која задовољава својства из друге дефиниције.

Убудуће ћемо чешће користити прву дефиницију, при чему ћемо знак операције $\cdot$ често изостављати (дакле писаћемо xy, а не $x \cdot y$), а и уместо „дата је група $(G, \cdot)$", писаћемо кратко „дата је група G". Осим тога, инверз елемента x обично ћемо записивати овако: x^{-1}.

Докажимо сада нека једноставна својства која следе из аксиома групе. Уведимо најпре једну помоћну ознаку. Производ $\prod_{i=1}^{n} x_i$ (где $x_i \in G$) дефинишемо рекурентном формулом

$$\prod_{i=1}^{n} x_i := e, \text{ ако је } n = 0,$$

$$\prod_{i=1}^{n+1} x_i := \prod_{i=1}^{n} x_i \cdot x_{n+1}, \text{ за } n \geq 0.$$

Посебно, ако је $x_1 = x_2 = \cdots = x_n = x$, уместо $\prod_{i=1}^{n} x$ пишемо x^n. Често ћемо уместо $\prod_{i=1}^{n} x_i$ писати $(x_1 \cdots x_n)$.

- За свако $n \geq 2$ и свако r, за које је $1 \leq r < n$ важи:

  $$(x_1 \cdots x_r) \cdot (x_{r+1} \cdots x_n) = (x_1 \cdots x_n).$$

  Ово заправо значи да заграде можемо произвољно да постављамо, па их ми често нећемо ни писати. Резултат се без тешкоћа доказује индукцијом по n. У случају да су сви x_i једнаки добијамо да је за све $m, n \in \mathbb{N}$: $x^m x^n = x^{m+n}$.

- За сваки $x \in G$:

  $$(x^{-1})^{-1} = x$$

  Овај резултат следи из јединствености инверза. Наиме, и елемент x и елемент $(x^{-1})^{-1}$ задовољавају услове за инверз елемента x^{-1}, па су стога једнаки.

- За све $x, y \in G$:

  $$(xy)^{-1} = y^{-1}x^{-1}.$$

  Обратите пажњу на редослед фактора! Проверимо да ли је $y^{-1}x^{-1}$ инверз елемента xy:

  $$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e,$$

  $$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e.$$

- Свака једначина облика

$$ax = b \qquad (*)$$

има тачно једно решење у G. То је тачно и за једначину облика

$$xa = b. \qquad (\circ)$$

Није тешко проверити да је $a^{-1}b$ једно решење једначине $(*)$:

$$a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Решење је јединствено: из $ax_1 = ax_2$ следи да је $a^{-1}ax_1 = a^{-1}ax_2$, тј. $ex_1 = ex_2$, па мора бити $x_1 = x_2$.

- За све $a, x \in G$ и $n \geq 1$:

$$(axa^{-1})^n = ax^n a^{-1}.$$

Доказ се изводи индукцијом по n.

Ако је $n = 1$, онда је тврђење тривијално тачно. Претпоставимо да је тврђење тачно за n и докажимо га за $n + 1$.

$$(axa^{-1})^{n+1} = \underbrace{(axa^{-1})^n(axa^{-1}) = ax^n a^{-1}axa^{-1}}_{\text{индуктивна хипотеза}} = ax^n xa^{-1} = ax^{n+1}a^{-1}.$$

Степен елемента x^m може се дефинисати и за негативне m:

$$x^{-n} := (x^{-1})^n, \text{ за } n \geq 1.$$

Наравно, ако је $n = 0$ узимамо $x^0 = e$. За вежбу доказати да важи:

- За свако $x \in G$ и свако $n \geq 1$: $x^{-n} = (x^n)^{-1}$.
- За свако $x \in G$ и све $m, n \in \mathbb{Z}$: $x^m x^n = x^{m+n}$.
- За свако $x \in G$ и све $m, n \in \mathbb{Z}$: $(x^m)^n = x^{mn}$.

Пређимо сада на примере група. Први и најједноставнији примери група су примери група које формирају бројеви. То су групе $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, а такође и $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{R}^+, \cdot)$, као и $(\mathbb{C} \setminus \{0\}, \cdot)$. Наравно, овде су $+$ и $\cdot$ уобичајене операције сабирања и множења бројева, док су са $\mathbb{Q}^+$ ($\mathbb{R}^+$) означени сви позитивни рационални (реални) бројеви. Но, наравно да појам групе није уведен због група које чине бројеви.

Посматрајмо неки правоугаоник, који није квадрат. Сем идентичне трансформације, он има још само три симетрије: две осне рефлексије (у односу на осе које су симетрале наспрамних страница) и једну централну рефлексију (у односу на центар правоугаоника). Јасно је

да композиција те две осне рефлексије даје централну. Означимо ову групу и њене елементе са

$$V = \{\varepsilon, \sigma_1, \sigma_2, \rho\},$$

где је са ε означена идентична трансформација, σ_1 и σ_2 су осне рефлексије, а ρ централна рефлексија. Није тешко саставити таблицу множења у овој групи.

$\circ$	ε	σ_1	σ_2	ρ
ε	ε	σ_1	σ_2	ρ
σ_1	σ_1	ε	ρ	σ_2
σ_2	σ_2	ρ	ε	σ_1
ρ	ρ	σ_2	σ_1	ε

Приметимо да за сваки елемент x ове групе важи: $x^2 = \varepsilon$ и да је група комутативна. Касније ћемо видети да из прве чињенице следи и друга. Група V зове се и Клајнова група.

Пређимо сада на сложеније примере.

Посматрајмо неки правилни многоугао у равни и потрудимо се да нађемо које све он симетрије има. У ту сврху, за почетак, није лоше посматрати неки конкретан случај и ми ћемо се концентрисати на два примера. На правилни петоугао и правилни шестоугао.

Симетрије које постоје у равни су: транслације, ротације, осне рефлексије и клизајуће рефлексије. Ако читалац није чуо за клизајуће рефлексије, то му ништа неће сметати. Наиме, клизајућа рефлексија је композиција једне транслације и једне осне рефлексије, па је довољно погледати шта се дешава са транслацијама и осним рефлексијама. Јасно је да транслације не долазе у обзир као симетрије неког многоугла. Слично се могу избацити и све ротације сем оне око центра многоугла. Наравно, не долазе у обзир ни све ротације око центра многоугла. У случају правилног n-тоугла, у „игри" су само ротације за углове облика $2k\pi/n$. Тако добијамо n различитих ротација, односно симетрија правилног n-тоугла. Дакле, у случају правилног петоугла имамо 5 ротација, док у случају правилног шестоугла имамо 6 ротација (не заборавимо да је ротација за угао $2n\pi/n$, односно ротација за угао 2π заправо идентична трансформација). Што се тиче осних рефлексија, ту је добро разликовати случај петоугла и шестоугла. У случају петоугла, имамо пет осних рефлексија и то око правих које пролазе кроз једно теме и средиште наспрамне странице. У случају правилног шестоугла имамо три рефлексије у односу на праве које пролазе кроз наспрамна темена и још три у односу на праве које пролазе кроз средишта наспрамних страница. Наравно, препоручујемо читаоцу да нацрта одговарајуће цртеже.

Означимо са ρ ротацију за угао $2\pi/n$ у смеру супротном кретању казаљке на часовнику. Видимо да су тада све ротације облика ρ^k за

неки k који може узимати вредности од 0 до $n-1$ (говоримо о правилном n-тоуглу). Приметимо да је $\rho^n = \varepsilon$. Са σ означимо било коју од наведених осних рефлексија. Није тешко проверити да је свака споменута рефлексија облика $\sigma\rho^k$ где је $0 \leq k < n$. Овде је добро разликовати случај парног и непарног n, односно једноставне случајеве правилног петоугла и правилног шестоугла. Приметимо да је $\sigma^2 = \varepsilon$. Посматрајмо скуп

$$\{\varepsilon, \rho, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}\}.$$

У односу на операцију композиције пресликавања, овај скуп представља групу. Та група има $2n$ елемената, назива се *диедарска* група и означава са $\mathbb{D}_n$.

Проверимо да је ово заиста група. Јасно је да је неутрал групе идентично пресликавање ε. Остаје нам да проверимо две ствари.

1) Да је композиција добро дефинисана на горенаведеном скупу.

2) Да сваки елемент из горенаведеног скупа има инверз.

Наиме, није јасно због чега, на пример, елемент $\rho\sigma$ припада том скупу. А и за многе друге композиције то није јасно. Испоставља се да је довољно да се провери колико је $\rho\sigma$; из тог резултата ће све следити.

Директном провером добија се да је

$$\rho\sigma = \sigma\rho^{n-1}.$$

Израчунајмо сада колико је $\rho^2\sigma$:

$$\rho^2\sigma = \rho\sigma\rho^{n-1} = \sigma\rho^{n-1}\rho^{n-1} = \sigma\rho^{2n-2} = \sigma\rho^{n-2}.$$

Није тешко добити и општи резултат:

$$\rho^k\sigma = \sigma\rho^{n-k}.$$

То се једноставно добија, на пример, индукцијом по k.

Приметимо да је заправо $\rho^{n-1} = \rho^{-1}$. То нам омогућава да горње идентитете запишемо на једноставнији начин:

$$\rho\sigma = \sigma\rho^{-1}; \quad \rho^k\sigma = \sigma\rho^{-k},$$

а имамо и

$$\sigma\rho^k = \rho^{-k}\sigma.$$

Сада се може проверити да је горњи скуп затворен у односу на композицију пресликавања.

$$\sigma\rho^k\rho^l = \begin{cases} \sigma\rho^{k+l}, & \text{ако је } k+l < n \\ \sigma\rho^{k+l-n}, & \text{ако је } k+l \geq n. \end{cases}$$

$$\sigma\rho^k\sigma\rho^l = \begin{cases} \rho^{-k+l}, & \text{ако је } k \leq l \\ \rho^{n-k+l}, & \text{ако је } k > l. \end{cases}$$

$$\rho^k\sigma\rho^l = \begin{cases} \sigma\rho^{-k+l}, & \text{ако је } k \leq l \\ \sigma\rho^{n-k+l}, & \text{ако је } k > l. \end{cases}$$

Наравно да је

$$\rho^k\rho^l = \begin{cases} \rho^{k+l}, & \text{ако је } k+l < n \\ \rho^{k+l-n}, & \text{ако је } k+l \geq n. \end{cases}$$

Занимљиво је написати целу таблицу множења за групу $\mathbb{D}_6$:

$\circ$	ε	ρ	ρ^2	ρ^3	ρ^4	ρ^5	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$
ε	ε	ρ	ρ^2	ρ^3	ρ^4	ρ^5	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$
ρ	ρ	ρ^2	ρ^3	ρ^4	ρ^5	ε	$\sigma\rho^5$	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$
ρ^2	ρ^2	ρ^3	ρ^4	ρ^5	ε	ρ	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$
ρ^3	ρ^3	ρ^4	ρ^5	ε	ρ	ρ^2	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$	$\sigma\rho^2$
ρ^4	ρ^4	ρ^5	ε	ρ	ρ^2	ρ^3	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$
ρ^5	ρ^5	ε	ρ	ρ^2	ρ^3	ρ^4	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ
σ	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	ε	ρ	ρ^2	ρ^3	ρ^4	ρ^5
$\sigma\rho$	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ	ρ^5	ε	ρ	ρ^2	ρ^3	ρ^4
$\sigma\rho^2$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$	ρ^4	ρ^5	ε	ρ	ρ^2	ρ^3
$\sigma\rho^3$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$	$\sigma\rho^2$	ρ^3	ρ^4	ρ^5	ε	ρ	ρ^2
$\sigma\rho^4$	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	ρ^2	ρ^3	ρ^4	ρ^5	ε	ρ
$\sigma\rho^5$	$\sigma\rho^5$	$\sigma\varepsilon$	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	ρ	ρ^2	ρ^3	ρ^4	ρ^5	ε

Било би добро да читаоци испишу таблице множења за групе $\mathbb{D}_3$, $\mathbb{D}_4$ и $\mathbb{D}_5$. Ако погледамо „горњи леви угао" наведене таблице, можемо да приметимо да се ту налази таблица множења у скупу $\{\varepsilon, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$. Заправо је то једна *подгрупа* групе $\mathbb{D}_6$.

Дефиниција 3 Ако су $(G, \cdot)$ и $(H, *)$ две групе, онда је група $(H, *)$ подгрупа групе $(G, \cdot)$ уколико је:

$$H \subseteq G \quad \text{и} \quad x * y = x \cdot y \text{ за све } x, y \in H.$$

Уколико је H подгрупа групе G, то записујемо овако: $H \leq G$.

Присетимо се да смо појам групе дефинисали на два еквивалентна начина — као структуру са само једном бинарном операцијом, односно као структуру са једном бинарном, једном унарном и једном нуларном операцијом. Уколико се присетимо појма подалгебре, знамо шта мора бити испуњено да би нека структура била подструктура друге. У нашем случају, изабрани елементи се морају поклапати, а такође и инверзи елемената из H морају бити једнаки инверзима тих елемената када се посматрају као елементи групе G. Дакле, ако је e неутрал у G, ε неутрал у H, x^{-1} инверз елемента $x \in G$, x' инверз елемента $x \in H$, онда мора бити:

- $e = \varepsilon$;
- за све $x \in H$: $x^{-1} = x'$.

Докажимо да је то заиста тако. Нека је $h \in H$ ма који елемент из H. Тада важи:

$$h * \varepsilon = h.$$

Но, тада је и

$$h \cdot \varepsilon = h,$$

пошто је $x \cdot y = x * y$ за све $x, y \in H$, а $h, \varepsilon \in H$. Множењем горње једнакости са h^{-1} добијамо

$$h^{-1} \cdot h \cdot \varepsilon = h^{-1} \cdot h,$$

а с обзимор да је $h^{-1} \cdot h = e$, следи

$$e \cdot \varepsilon = e,$$

те је заиста $\varepsilon = e$.

Да бисмо доказали да је за све $x \in H$ испуњено $x^{-1} = x'$, напишимо шта значи то да је x^{-1} инверз елемента x у G и да је x' инверз елемента x у H (елемент x припада H):

$$x \cdot x^{-1} = x^{-1} \cdot x = e, \qquad (1)$$

$$x * x' = x' * x = \varepsilon. \qquad (2)$$

Но, с обзиром да x, x' припадају H и да је $e = \varepsilon$, добијамо да је

$$x \cdot x' = x' \cdot x = e. \qquad (3)$$

Из (1) и (3) на основу јединствености инверза у групи добијамо да мора бити $x' = x^{-1}$.

Наведимо сада један користан став.

Став 4 Непразан скуп H групе G је подгрупа групе G у односу на рестрикцију операције из G ако и само ако је $xy^{-1} \in H$ за све $x, y \in H$.

Доказ. Јасно је да свака подгрупа задовољава наведено својство. Наиме, ако су $x, y \in H$, како је H подгрупа, то и $y^{-1} \in H$. Осим тога, операција у H је заправо рестрикција операције у G, па мора бити $xy^{-1} \in H$, пошто $x \in H$ и $y^{-1} \in H$.

Претпоставимо да је H непразан скуп и да задовољава тражени услов. Како је $H \neq \emptyset$, то постоји $h \in H$. Тада по претпоставци и $e = hh^{-1} \in H$. Ако је $x \in H$ произвољан, из претпоставке и чињенице да $e \in H$, следи да и $x^{-1} = ex^{-1}$ такође припада H. Коначно, ако су $x, y \in H$, онда по већ доказаном, $y^{-1} \in H$, па је и $xy = x(y^{-1})^{-1} \in H$. □

Став 5 Ако су H и K подгрупе групе G, онда је $H \cap K$ подгрупа групе G, док је $H \cup K$ подгрупа групе G ако и само ако је $H \subseteq K$ или $K \subseteq H$.

Доказ. Докажимо најпре да је пресек две подгрупе такође подгрупа. Како и H и K морају садржати неутрал, то је $H \cap K \neq \emptyset$. Претпоставимо да $x, y \in H \cap K$. То значи да $x, y \in H$ и $x, y \in K$. На основу раније доказаног, $xy^{-1} \in H$ и $xy^{-1} \in K$, па $xy^{-1} \in H \cap K$. Закључујемо да је $H \cap K$ подгрупа групе G.

Позабавимо се унијом две подгрупе. Јасно је да ако је једна од њих подскуп друге, њихова унија се поклапа са једном од њих, те јесте подгрупа групе G. Претпоставимо да је $H \cup K$ подгрупа групе G и нека $H \not\subseteq K$. Доказаћемо да је $K \subseteq H$. Како $H \not\subseteq K$, то постоји елемент h који јесте у H, а није у K. Узмимо произвољни елемент $k \in K$. Доказаћемо да је он у H и тиме показати да је $K \subseteq H$. Посматрајмо елемент $k \cdot h$. Како су и k и h из $K \cup H$, а $K \cup H$ је подгрупа групе G, то сигурно $k \cdot h \in K \cup H$. Но, ако $k \cdot h \in K$, користећи чињеницу да k припада K, добијамо да је и $h = k^{-1}kh$ из K, а то није могуће. Дакле, $k \cdot h$ мора бити у H, па како је $h \in H$ и $k = kh \cdot h^{-1}$, то $k \in H$. □

На сличан начин се може показати да је пресек произвољне фамилије подгрупа неке групе такође подгрупа те групе. Наиме, нека су H_i подгрупе од G, где $i \in I$. Како за све $i \in I$ неутрал e припада H_i, то је

$$\bigcap_{i \in I} H_i \neq \emptyset.$$

Нека $x, y \in \bigcap_{i \in I} H_i$. Тада за све $i \in I$: $x \in H_i$ и $y \in H_i$. Како су H_i подгрупе, то $xy^{-1} \in H_i$, за све $i \in I$, те заиста $xy^{-1} \in \bigcap_{i \in I} H_i$.

Стога има смисла следеће питање.

Питање: Ако је G група и X подскуп те групе, да ли постоји најмања подгрупа групе G, која садржи X (као свој подскуп)?

Одговор је потврдан—то је пресек свих подгрупа које садрже X. Наиме, сигурно постоји бар једна подгрупа групе G, која садрхи X (сама група G!), па има смисла говорити о пресеку. Најмања подгрупа која садржи X означава се са $\langle X \rangle$ и зове се *подгрупа генерисана скупом* X. Скуп X је скуп генератора те групе. Уколико је $X = \emptyset$, онда је $\langle X \rangle = \{e\}$. Уколико је $X = \{a\}$, онда је $\langle X \rangle$ *циклична подгрупа* генерисана елементом a и означавамо је са $\langle a \rangle$.

Вратимо се диедарској групи $\mathbb{D}_n$. Ако је $X = \{\rho, \sigma\}$, шта је $\langle X \rangle$? Јасно је да је заправо $\langle X \rangle = \mathbb{D}_n$. Дакле, група $\mathbb{D}_n$ је генерисана са два генератора.

Ако са X^{-1} означимо скуп свих инверза елемената из X,

$$X^{-1} = \{x^{-1} : x \in X\},$$

онда није тешко показати да је

$$\langle X\rangle = \{a_1 \cdots a_n : n \in \mathbb{N}, a_i \in X \cup X^{-1}\}.$$

(у случају да је $n = 0$, производ $a_1 \cdots a_n$ је наравно неутрал e). Наиме, ако су $a_1 \cdots a_n$ и $b_1 \cdots b_m$ производи елемената из $X \cup X^{-1}$, јасно је да је то и

$$a_1 \cdots a_n \cdot (b_1 \cdots b_m)^{-1} = a_1 \cdots a_n \cdot b_m^{-1} \cdots b_1^{-1}.$$

Стога скуп са десне стране горње једнакости заиста чини подгрупу у односу на рестрикцију операције, а јасно је да свака подгрупа H за коју је $X \subset H$ мора садржати тај скуп као свој подскуп. Према томе, заиста је то најмања подгрупа која садржи скуп X као свој подскуп.

Приметимо на крају да, мада се став **??** може проширити у случају пресека на произвољну колекцију подскупова, то се не може урадити за уније. Једноставан пример нам даје Клајнова група V. Наиме, $H_1 = \{\varepsilon, \sigma_1\}$, $H_2 = \{\varepsilon, \sigma_2\}$ и $H_3 = \{\varepsilon, \rho\}$, су подгрупе од V и за њих важи:

$$V = H_1 \cup H_2 \cup H_3,$$

а ниједна од њих није садржана у некој другој.

Цикличне групе; изоморфизми група

Видели смо да је $\{\varepsilon, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$ једна подгрупа групе $\mathbb{D}_6$. Приметимо да је у овој групи сваки елемент облика ρ^k за неки цео број k. Групе са овим својством називају се цикличне групе.

Дефиниција 6 Група G је *циклична* група уколико постоји елемент $x \in G$ такав да је сваки елемент из G облика x^m за неки цео број m, односно

$$G = \{x^m : m \in \mathbb{Z}\}.$$

Такав елемент зовемо генератор цикличне групе.

У складу са дефиницијом групе генерисане неким подскупом, циклична група је она група која је генерисана једночланим подскупом, тј. једним елементом. Уколико желимо да истакнемо да је G циклична група чији је генератор a, онда то пишемо овако: $G = \langle a\rangle$.

Група ротација правилног n-тоугла, је такође циклична група и она је генерисана ротацијом за угао $2\pi/n$. Наведимо још неке примере цикличних група.

- $\mathbb{Z}_n = (Z_n, +_n)$ је циклична група генерисана елементом 1. Овде је $+_n$ сабирање по модулу n, а $Z_n = \{0, 1, \ldots, n-1\}$, где је $n \geq 2$.

- $\mathbb{C}_n = \{z \in \mathbb{C} : z^n = 1\}$ је такође циклична група у односу на множење комплексних бројева. То је група свих n-тих корена из јединице и генерисана је елементом $e^{2i\pi/n} (= \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})$. Генератор те групе се зове и *примитивни* n-ти корен из јединице.
- $(\mathbb{Z}, +)$ је циклична група генерисана елементом 1.

Приметимо да постоје и цикличне групе са коначно много елемената, као и цикличне групе са бесконачно много елемената. Заправо за сваки природан број $n \geq 1$ постоји циклична група са n елемената (у случају да је $n = 1$ добијамо тривијалну групу чији је једини елемент неутрал). Природно се поставља питање: да ли су две цикличне групе са истим бројем елемената суштински различите? Испоставља се да је одговор негативан — сваке две цикличне групе са истим бројем елемената су изоморфне, али ће више речи о томе бити на крају ове лекције.

Уводимо сада појам реда групе и реда елемента групе.

Дефиниција 7 Ако је група G коначна онда број њених елемената зовемо ред групе и означавамо са $|G|$. У случају да је група бесконачна, кажемо да је она бесконачног реда.

Нека је a елемент неке групе. Уколико не постоји природан број $n \geq 1$ за који је $a^n = e$, кажемо да је елемент a бесконачног реда. Уколико такав елемент постоји, онда је ред елемента a, у ознаци $\omega(a)$ задат са:

$$\omega(a) := \min\{m \geq 1 : a^m = e\}.$$

Став 8 Ред ма ког елемента неке групе једнак је реду подгрупе генерисане тим елементом.

Доказ. Уколико је елемент a бесконачног реда, онда је $a^k \neq a^l$ за све $k \neq l$. Наиме, ако је $a^k = a^l$ за неке k и l при чему је $k > l$, онда је $a^{k-l} = e$, а $k - l \geq 1$, што противречи претпоставци да је a бесконачног реда. Но, из чињенице да је $a^k \neq a^l$ за $k \neq l$ следи да је подгрупа $\langle a \rangle$ бесконачна.

Дакле, елемент бесконачног реда генерише бесконачну подгрупу. Обратно, ако је подгрупа генерисана елементом a бесконачна онда елемент a мора бити бесконачног реда. Претпоставимо да је $\omega(a) = n \geq 1$. Тврдимо да је тада

$$\langle a \rangle = \{e, \ldots, a^{n-1}\}$$

и да су сви ови елементи различити. Наиме, сваки елемент из $\langle a \rangle$ је облика a^m за неки цео број m. Поделимо са остатком m са n. Добијамо да је $m = qn + r$, где је $0 \leq r < n$. Тада је

$$a^m = (a^n)^q a^r = e^q a^r = a^r \in \{e, \ldots, a^{n-1}\}.$$

Закључујемо да је $\langle a \rangle = \{e, \ldots, a^{n-1}\}$. Уколико би било $a^r = a^s$ за неке $0 \leq r < s < n$, онда би важило и $a^{s-r} = e$, а то није могуће, јер

је $0 < s - r < n$, а $n = \omega(n)$. Закључујемо да су сви ови елементи различити, те је ред те подгрупе заиста n, а то је и ред елемента a. □

Став 9 Ако је елемент a бесконачног реда и $m \neq 0$, онда је и a^m бесконачног реда. Уколико је $\omega(a) = n$ и $m \neq 0$ онда је

$$\omega(a^m) = \frac{n}{\text{NZD}(m, n)}.$$

Доказ. Први део тврђења се лако доказује. Наиме, ако је $(a^m)^r = e$, онда је и $a^{mr} = e$, па би и a био коначног реда. Доказ другог дела је тежи.

Нека је $d = \text{NZD}(m, n)$. Тада је $m = m_1 d$ и $n = n_1 d$, при чему су m_1 и n_1 узајамно прости. Ми треба да докажемо да је $\omega(a^m) = n_1$.

$$(a^m)^{n_1} = a^{mn_1} = a^{m_1 d n_1} = a^{m_1 n} = (a^n)^{m_1} = e^{m_1} = e.$$

Претпоставимо да је $k > 0$ такав да је $(a^m)^k = e$. Треба да покажемо да је $n_1 \leq k$. Дакле, $a^{mk} = e$ и $a^n = e$ (пошто је $n = \omega(a)$). Постоје цели бројеви q и r такви да је $mk = qn + r$, где је $0 \leq r < n$. Добијамо да је $a^{mk} = (a^n)^q a^r$, те следи да је $a^r = e$. Но, $n = \omega(a)$ и $0 \leq r < n$, па мора бити $r = 0$. Дакле, $n \mid mk$. Добијамо $dn_1 \mid dm_1 k$, па $n_1 \mid m_1 k$. Како су m_1 и n_1 узајамно прости добијамо да $n_1 \mid k$, па мора бити $n_1 \leq k$, што се и тражило. □

Напомена. Приметимо да се у овом доказу „крије" и доказ следећег резултата: ако је n ред елемента a, онда за сваки $l \in \mathbb{Z}$ важи

$$a^l = e \text{ ако и само ако } n \mid l.$$

Како је овај резултат од посебног значаја, даћемо и његов комплетан доказ.

- Претпоставимо да је $n = \omega(a)$ и да је $a^l = e$. Поделимо l са n. Добијамо да је $l = qn + r$, где је $0 \leq r < n$. Но, тада је

  $$e = a^l = a^{qn+r} = (a^n)^q \cdot a^r = e^q \cdot a^r,$$

  те добијамо да је $a^r = e$. Како је $0 \leq r < n = \omega(a)$, то је могуће једино ако је $r = 0$. Дакле, $n \mid l$.

- Нека $n \mid l$. Тада је $l = qn$, за неки цео број q и добијамо

  $$a^l = a^{qn} = (a^n)^q = e^q = e.$$

Пример 10 Одредити ред елемента 18 у групи $\mathbb{Z}_{120}$.

Решење. Како је 1 генератор групе $\mathbb{Z}_{120}$,

$$18 = \underbrace{1 + \cdots + 1}_{18}$$

и $\text{NZD}(18, 120) = 6$, то је ред елемента 18 једнак $\frac{120}{6} = 20$. ♣

Докажимо сада теорему о подгрупама цикличне групе.

Теорема 11 1) Свака подгрупа цикличне групе и сама је циклична.
2) Ако је G циклична група коначног реда n и ако $k \mid n$, онда постоји тачно једна подгрупа H групе G, која је реда k.

Доказ. 1) Нека је $G = \langle a \rangle$ и $H \leq G$. Ако је $H = \{e\}$, немамо шта да доказујемо. У супротном нека је $s = \min\{n > 0 : a^n \in H\}$. Показаћемо да је $H = \langle a^s \rangle$. Како је $a^s \in H$, то је и $(a^s)^m \in H$ за све $m \in \mathbb{Z}$, па је $\langle a^s \rangle \subseteq H$.

Претпоставимо да $x \in H$. Како је G циклична група, то је $x = a^k$ за неки цео број k. Тада постоје цели бројеви q и r за које је $k = qs + r$, при чему је $0 \leq r < s$. Дакле, $r = k - qs$ и добијамо $a^r = a^k(a^s)^{-k}$. Како је $a^k = x \in H$ и $a^s \in H$, то следи да $a^r \in H$. Но, $0 \leq r < s$ и по избору броја s мора бити $r = 0$. Дакле, $x = a^k = (a^s)^q \in \langle a^s \rangle$.

2) Како је $\omega(a) = n$ и $k \mid n$, то је према претходном ставу $\omega(a^{n/k}) = k$ и подгрупа H, генерисана елементом $a^{n/k}$ је реда k. Претпоставимо да постоји још једна подгрупа H_1 истог реда k. Како је, према већ доказаном, подгрупа H_1 циклична, онда је $H_1 = \langle a^l \rangle$. Како је $\omega(a^l) = |H_1| = k$, то је $(a^l)^k = e$. Дакле, $a^{kl} = e$, а $\omega(a) = n$, па добијамо да $n \mid kl$. Како $k \mid n$, добијамо да $\frac{n}{k} \mid l$, те је $l = \frac{n}{k} l_1$ за неко l_1. Но, тада је $a^l = (a^{n/k})^{l_1} \in H$ и $H_1 \subseteq H$. Како је $|H_1| = k = |H|$, то је $H_1 = H$ и тражена подгрупа је заиста јединствена. □

Пример 12 Одредити јединствену подгрупу H реда 6 у групи $\mathbb{Z}_{18}$.

Решење. Како је $18/6 = 3$, то је тражена подгрупа H генерисана елементом 3 и $H = \{0, 3, 6, 9, 12, 15\}$. Напишимо и таблицу сабирања у тој подгрупи.

$+_{18}$	0	3	6	9	12	15
0	0	3	6	9	12	15
3	3	6	9	12	15	0
6	6	9	12	15	0	3
9	9	12	15	0	3	6
12	12	15	0	3	6	9
15	15	0	3	6	9	12

♣

Упоредите ову таблицу са таблицом сабирања у групи $\mathbb{Z}_6$.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Евидентно је да ове таблице врло слично изгледају. То није случајно.

Пређимо сада на појам изоморфизма група.

Дефиниција 13 Нека су $(G, \cdot)$ и $(H, *)$ групе. Кажемо да су ове групе изоморфне уколико постоји бијекција $f: G \to H$ таква да је за све $x, y \in G$:

$$f(x \cdot y) = f(x) * f(y).$$

Бијекција из ове дефиниције зове се изоморфизам група G и H. Чињеницу да је група G изоморфна групи H записујемо овако: $G \cong H$.

Уколико је e неутрал у G, а ε неутрал у H и $f: G \to H$ изоморфизам, важи следеће:

- $f(e) = \varepsilon$;
- $f(x^{-1}) = f(x)^{-1}$.

Наиме, $f(e) = f(e \cdot e) = f(e) * f(e)$, те следи да је $f(e) = \varepsilon$. Слично, $\varepsilon = f(e) = f(x \cdot x^{-1}) = f(x) * f(x^{-1})$, па закључујемо да је $f(x^{-1}) = f(x)^{-1}$.

Став 14 Ако је $f: G \to H$ изоморфизам група, онда је и $f^{-1}: H \to G$, такође изоморфизам.

Доказ. Јасно је да $f^{-1} : H \to G$ постоји, пошто је f бијекција. Треба показати да је $f^{-1}(u * v) = f^{-1}(u) \cdot f^{-1}(v)$ за све $u, v \in H$. Како је f „на", то постоје x и y тако да је $u = f(x)$ и $v = f(y)$. Но, тада је

$$f^{-1}(u * v) = f^{-1}(f(x) * f(y)) = f^{-1}(f(x \cdot y)) =$$

$$= (f^{-1} \circ f)(x \cdot y) = \mathrm{id}_G(x \cdot y) = x \cdot y = f^{-1}(u) \cdot f^{-1}(v).$$

□

Изоморфизам чува ред елемента у групи.

Став 15 Ако је $f: G \to H$ изоморфизам и $x \in G$, онда је $\omega(f(x)) = \omega(x)$.

Доказ. Размотримо најпре случај када је x бесконачног реда. Покажимо да је и $f(x)$ такође бесконачног реда. У супротном, је $(f(x))^n = \varepsilon$ за неко $n > 0$. Но, тада је $f(x^n) = f(e)$, а како је f „1–1" закључујемо

да је $x^n = e$, што противречи претпоставци да је x бесконачног реда. Закључујемо да да је и $f(x)$ бесконачног реда.

Нека је $n = \omega(x)$. Тада је $f(x)^n = f(x^n) = f(e) = \varepsilon$, па добијамо да је и $f(x)$ коначног реда m и да $m \mid n$. Но, $x^m = (f^{-1}(f(x)))^m = f^{-1}(f(x)^m) = f^{-1}(\varepsilon) = e$, па $n \mid m$. Дакле, $m = n$. □

Напомена. Овде смо искористили раније доказани резултат да је за елемент z неке групе испуњено: $z^n = e$ ако и само ако $\omega(z) \mid n$.

Заправо, две изоморфне групе су потпуно идентичне по својим алгебарским својствима; једино се могу разликовати по природи својих елемената.

Сада можемо да докажемо следећу теорему.

Теорема 16 Свака циклична група изоморфна је или групи $\mathbb{Z}$ или групи $\mathbb{Z}_n$ за неко $n \geq 1$.

Доказ. Претпоставимо најпре да је G бесконачна циклична група. То значи да постоји елемент $a \in G$ такав да је

$$G = \{a^m : m \in \mathbb{Z}\}.$$

Осим тога, $a^k \neq a^l$ уколико је $k \neq l$. У овом случају дефинишимо $f{:}\mathbb{Z} \to G$ са: $f(m) = a^m$. Јасно је да је f бијекција (зашто?). Треба само проверити да је $f(m+n) = f(m) \cdot f(n)$ за све $m, n \in \mathbb{Z}$. Но, то је заправо раније наведено својство: $a^{m+n} = a^m \cdot a^n$. Закључујемо да је у овом случају $G \cong \mathbb{Z}$.

Претпоставимо да је G коначна циклична група, тј. да је за неки елемент $a \in G$

$$G = \{e, a, \ldots, a^{n-1}\},$$

за неки природан број $n \geq 2$ (случај $n = 1$ је једноставан, ту добијамо само тривијалну групу $\{e\}$). Доказаћемо да је у овом случају $G \cong \mathbb{Z}_n$. Дефинишемо функцију $f{:}\mathbb{Z}_n \to G$ са: $f(k) := a^k$. Као и у претходном случају, јасно је да је f бијекција. Треба само показати да је

$$f(k +_n l) = f(k) \cdot f(l).$$

Подсетимо се да је, за $k, l \in \{0, 1, \ldots, n-1\}$:

$$k +_n l = \begin{cases} k + l, & k + l < n \\ k + l - n, & k + l \geq n. \end{cases}$$

Уколико је $k + l < n$, добијамо да је

$$f(k) \cdot f(l) = a^k \cdot a^l = a^{k+l} = f(k+l) = f(k +_n l).$$

У случају да је $k + l \geq n$,

$$f(k) \cdot f(l) = a^k \cdot a^l = a^{k+l} = a^{(k+_n l)+n} = a^{k+_n l} \cdot a^n = a^{k+_n l} \cdot e = a^{k+_n l} = f(k +_n l).$$

Дакле, f је заиста изоморфизам и закључујемо да је $\mathbb{Z}_n \cong G$. □

Сада знамо да је јединствена подгрупа реда 6 у групи $\mathbb{Z}_{18}$, чију смо таблицу сабирања раније записали, изоморфна групи $\mathbb{Z}_6$, што објашњава сличност њихових таблица сабирања.

Групе пермутација

У овој лекцији обрађујемо веома значајан пример групе — групу пермутација (групу симетрија).

Дефиниција 17 Нека је X непразан скуп. Посматрајмо скуп S_X задат са:

$$S_X = \{\pi \colon X \to X \mid \pi \text{ је бијекција } \}.$$

Тада је $\mathbb{S}_X = (S_X, \circ)$, где је са $\circ$ означена операција композиције функција, једна група и зовемо је групом пермутација скупа X.

Елементе групе $\mathbb{S}_X$ зовемо и пермутацијама скупа X. Ако постоји бијекција између X и Y, онда су одговарајуће групе пермутација изоморфне.

Став 18 Ако постоји бијекција између X и Y, онда је $\mathbb{S}_X \cong \mathbb{S}_Y$.

Доказ. Нека је $g \colon X \to Y$ бијекција. Дефинишимо $f \colon S_X \to S_Y$ са:

$$f(\pi) := g \circ \pi \circ g^{-1}.$$

Јасно је да је $g \circ \pi \circ g^{-1}$ једна пермутација скупа Y уколико је π пермутација скупа X. Осим тога, ако је $\sigma \in S_Y$, онда је $f(g^{-1} \circ \sigma \circ g) = \sigma$, те је f „на". Јасно је да је f и „1–1". Треба само проверити да је $f(\rho \circ \pi) = f(\rho) \circ f(\pi)$, уколико $\rho, \pi \in S_X$. Учинимо то:

$$f(\rho \circ \pi) = g \circ (\rho \circ \pi) \circ g^{-1} = (g \circ \rho \circ g^{-1}) \circ (g \circ \pi \circ g^{-1}) = f(\rho) \circ f(\pi).$$

Дакле, f заиста успоставља изоморфизам између $\mathbb{S}_X$ и $\mathbb{S}_Y$. □

Уколико је $X = \{1, 2, \ldots, n\}$, онда уместо $\mathbb{S}_{\{1,2,\ldots,n\}}$ пишемо краће $\mathbb{S}_n$. На основу претходног става, свака коначна група пермутација неког скупа изоморфна је једној од група $\mathbb{S}_n$. Стога се сада концентришемо на групу $\mathbb{S}_n$.

Почнимо једним примером. Нека је $n = 9$ и пермутација $\sigma \in \mathbb{S}_9$ задата са:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 3 & 8 & 2 & 7 & 1 & 6 & 9 \end{pmatrix}.$$

Можемо ли ову пермутацију некако једноставније записати? Елемент 1 слика се у 4, 4 у 8, 8 у 6, 6 у 7, а 7 у 1. Некако смо „затворили круг”:

$$1 \mapsto 4 \mapsto 8 \mapsto 6 \mapsto 7 \mapsto 1.$$

Запишимо то овако: (14867). Прецизније, (14867) означава пермутацију скупа $\{1, 2, \ldots, 9\}$ у којој се 1 слика у 4, 4 у 8, 8 у 6, 6 у 7, а 7 у 1, док се остали елементи сликају сами у себе. Како се остали елементи не појављују у овом запису, а сликају се сами у себе, то се (14867) може видети и као елемент групе S_n за ма које $n \geq 8$. Оваква пермутација назива се циклус или цикл дужине 5. Пермутација у којој

$$a_1 \mapsto a_2 \mapsto \cdots \mapsto a_{k-1} \mapsto a_k \mapsto a_1,$$

при чему су елементи a_i различити, означава се са $(a_1 a_2 \ldots a_k)$, зове се циклус дужине k (или k-цикл).

Вратимо се пермутацији σ. Први елемент који нисмо „покупили” до сада је елемент 2. Видимо да

$$2 \mapsto 5 \mapsto 2.$$

Дакле, добијамо нови цикл (25), који је дужине 2. Цикли дужине 2 зову се и транспозиције (само два елемента замене своја места). Видимо да се преостали елементи 3 и 9 не померају при пермутацији σ: $3 \mapsto 3$, односно $9 \mapsto 9$. То се може записати и у облику циклуса дужине 1: (3), односно (9). Но, то су, по нашој дефиницији, заправо идентичне пермутације (3 се слика у 3, а остали такође сами у себе!), те их често и не пишемо. Проверимо да ли је

$$\sigma = (14867)(25).$$

Овде треба напоменути да знак за композицију $\circ$ најчешће нећемо писати. Осим тога, подсетимо читаоца да су ово функције, те ова ознака значи да прво делује (25), а потом (14867). Није тешко проверити да горња једнакост заиста важи. Овако смо нашу пермутацију приказали о облику производа дисјунктних циклуса (циклуси $(a_1 a_2 \ldots a_k)$ и $(b_1 b_2 \ldots b_l)$ су дисјунктни уколико су $\{a_1, a_2, \ldots, a_k\}$ и $\{b_1, b_2, \ldots, b_l\}$ дисјунктни скупови). Заправо важи следећа теорема.

Теорема 19 Свака пермутација из $\mathbb{S}_n$ може се на јединствен начин, до на редослед фактора, представити у облику производа дисјунктних циклуса.

Ову теорему нећемо доказивати. Приметимо да важи следеће. Уколико су циклуси ρ и π дисјунктни, онда је $\rho\pi = \pi\rho$. То није тешко директно проверити анализирајући где се сликају поједини елементи.

Уколико пак циклуси нису дисјунктни, они не морају да комутирају:

$$(12)(23) = (123), \quad (23)(12) = (132).$$

Приметимо да је

$$(a_1a_2\dots a_k) = (a_2\dots a_ka_1) = \dots = (a_k\dots a_1a_2\dots a_{k-1}).$$

У конкретном случају $k = 4$:

$$(a_1a_2a_3a_4) = (a_2a_3a_4a_1) = (a_3a_4a_1a_2) = (a_4a_1a_2a_3).$$

У вези са овим, природно се поставља питање колико у S_n има различитих циклуса дужине k, где је $k \leq n$. На то питање није тешко одговорити. Наиме, најпре је потребно из скупа од n елемената изабрати њих k. То се може извести на $\binom{n}{k}$ начина. Ти елементи се међусобно могу поређати у циклус дужине k на $k!$ начина. Но, видели смо да неке од тих пермутација заправо задају исти циклус. Прецизније, од датих k елемената може се формирати $\frac{k!}{k} = (k-1)!$ различитих циклуса. Дакле, различитих циклуса дужине k у S_n има $\binom{n}{k}(k-1)! = \frac{n(n-1)\cdots(n-k+1)}{k}$. Наравно, ово се може доказати и на друге начине. Размислите како.

Позабавимо се мало рачунањем са циклусима. Најпре, лако је проверити да је, ако су a, b, c међусобно различити, $(ab)(bc) = (abc)$. Општији резултат је следећи. Ако су $a_1, a_2, \dots, a_{k+l}$ међусобно различити онда је:

$$(a_1a_2\dots a_k)(a_ka_{k+1}\dots a_{k+l}) = (a_1a_2\dots a_{k+l}),$$

за све $k \geq 2, l \geq 1$. Користећи овај резултат, лако се показује да је сваки циклус производ транспозиција:

$$(a_1a_2)(a_2a_3)\cdots(a_{k-1}a_k) = (a_1a_2\dots a_k).$$

Како је свака пермутација производ циклуса то закључујемо да важи следећи став.

Став 20 Свака пермутација из $\mathbb{S}_n$ може се представити у облику производа транспозиција.

Овде треба истаћи да представљање није јединствено. Нпр.

$$(12)(23)(34) = (14)(13)(12).$$

Оно што јесте јединствено је парност броја транспозиција које се појављују у факторизацији дате пермутације. Тај резултат такође нећемо доказивати. Укажимо само да пермутације које се могу представити у облику производа парног броја транспозиција зовемо парне пермутације, док се пермутације које се представљају у облику непарног броја транспозиција зову непарне пермутације. Скуп свих парних пермутација чини групу. Та група се означава са $\mathbb{A}_n$ и важи следећи став.

Став 21 За свако $n \geq 2$ је $\mathbb{A}_n \leq \mathbb{S}_n$ и $|\mathbb{A}_n| = \frac{n!}{2}$.

Доказ. Како је идентична пермутација очигледно парна (зашто?), то је $A_n \neq \emptyset$. Осим тога, ако су σ и π парне пермутације, то је и $\sigma\pi^{-1}$ парна пермутација. Наиме, ако је $\sigma = \tau_1\tau_2\cdots\tau_{2k}$, а $\pi = \phi_1\phi_2\cdots\phi_{2l}$, представљање ових пермутација у облику производа парног броја транспозиција то је $\sigma\pi^{-1} = \tau_1\tau_2\cdots\tau_{2k}\phi_{2l}\cdots\phi_2\phi_1$ представљање у облику производа парног броја транспозиција (појаснити ову последњу једнакост). Стога закључујемо да је $\mathbb{A}_n$ заиста подгрупа групе $\mathbb{S}_n$.

Да бисмо одредили ред подгрупе $\mathbb{A}_n$, изаберимо било коју транспозицију τ. Тада можемо дефинисати функцију $\Phi\colon A_n \to S_n \setminus A_n$ са: $\Phi(\pi) := \tau\pi$. Није тешко уверити се да је Φ бијекција. Резултат одавде следи (проверити да је Φ бијекција и објаснити како се добија тражени резултат). □

Ако је $\pi \in \mathbb{S}_n$ и $(a_1a_2\ldots a_k)$ један k-цикл тада је

$$\pi(a_1a_2\ldots a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)\ldots\pi(a_k)).$$

Ово се лако може проверити. Споменимо узгред да је

$$(a_1a_2\ldots a_k)^{-1} = (a_ka_{k-1}\ldots a_1).$$

Видели смо да је група $\mathbb{S}_n$ генерисана транспозицијама. То је прилично велики генераторни скуп. Заправо се могу наћи знатно једноставнији скупови генератора за $\mathbb{S}_n$.

Став 22 Група $\mathbb{S}_n$ генерисана је:

1. транспозицијама $(12), (13), \ldots, (1n)$;
2. транспозицијама $(12), (23), (34), \ldots (n-1, n)$;
3. пермутацијама (12) и $(123\ldots n)$.

Доказ.
1. Лако се може проверити да је $(ab) = (1a)(1b)(1a)$. Дакле, све транспозиције се могу добити помоћу наведених.

2. Довољно је показати да можемо да добијемо све транспозиције облика $(1a)$ за $2 \leq a \leq n$. Наравно, (12) је већ на списку! Ево како добијамо (13):

$$(13) = (12)(23)(12).$$

Сада када имамо (13) није тешко добити и (14):

$$(14) = (13)(34)(13).$$

Уочавамо правилност:

$$(1, k+1) = (1k)(k, k+1)(1k).$$

На овај начин добијамо све транспозиције за које знамо да генеришу $\mathbb{S}_n$. Стога и почетне транспозиције генеришу $\mathbb{S}_n$.

3. Подсетимо се формуле: $\pi(a_1 \dots a_k)\pi^{-1} = (\pi(a_1) \dots \pi(a_k))$ (**веома** пажљив читалац је можда приметио да се ова формула крије и у идентитету $(13) = (12)(23)(12)$). Уколико је $\pi = (12 \dots n)$ добијамо

$$(12 \dots n)(12)(12 \dots n)^{-1} = (23).$$

Када смо добили (23), није нам тешко да добијемо и (34):

$$(12 \dots n)(23)(12 \dots n)^{-1} = (34).$$

Уочавамо правилност:

$$(12 \dots n)(k, k+1)(12 \dots n)^{-1} = (k+1, k+2),$$

за $1 \leq k \leq n-2$. Тако добијамо све транспозиције за које знамо да генеришу $\mathbb{S}_n$, па према томе закључујемо да и дате две пермутације такође генеришу $\mathbb{S}_n$. □

Приметимо да парност k-цикла зависи од k. Заправо је k-цикл парна пермутација ако и само ако је k непаран (погледајте како смо k-цикл представили у облику производа транспозиција). То посебно значи да је сваки цикл дужине три (трицикл!) једна парна пермутација. Важи следећи став.

Став 23 Ако је $n \geq 3$, онда је $\mathbb{A}_n$ генерисана циклусима дужине 3.

Доказ. Ово заправо није тешко доказати. Уколико је $n = 3$ и немамо шта да доказујемо. Наиме, $\mathbb{S}_3 = \{(1), (12), (13), (23), (123), (132)\}$ ((1) представља идентичну пермутацију). Дакле, овде је заправо $\mathbb{A}_3 = \{(1), (123), (132)\}$. Претпоставимо стога да је $n \geq 4$. Како је, према претходном ставу, скуп $\{(12), (13), \dots, (1n)\}$ један скуп генератора групе $\mathbb{S}_n$, то се и сваки елемент из $\mathbb{A}_n$ може представити у облику производа ових елемената. Но, како је у питању елемент из $\mathbb{A}_n$, он је представљен у облику производа парног броја таквих транспозиција. Групишући их две по две, добијамо да је довољно да покажемо да се пермутације облика $(1a)(1b)$, где је $a \neq b$ могу представити у облику производа циклуса дужине 3. Но, заправо је $(1a)(1b) = (a1)(1b) = (a1b)$! Дакле, то је већ циклус дужине 3. Овим је доказ завршен. □

Позабавимо се сада питањем одређивања реда елемената из $\mathbb{S}_n$. Директном провером се добија да је $\omega((a_1 \dots a_k)) = k$. Како се свака пермутација може представити у облику производа дисјунктних циклуса, то би морало бити корисно за одређивање реда произвољне пермутације. Доказаћемо један општи став.

Став 24 Нека је G произвољна група и $a, b \in G$ такви да је:

1. $\omega(a) = m$, $\omega(b) = n$;
2. $ab = ba$;
3. $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Тада је $\omega(ab) = \text{NZS}(m, n)$.

Доказ. Како је $ab = ba$, то је за сваки $k \in \mathbb{N}$: $(ab)^k = a^k b^k$. То се лако доказује индукцијом (докажите то за вежбу!). Ради краћег записа уведимо ознаке: $s = \omega(ab)$, $t = \text{NZS}(m, n)$. Осим тога, $t = mt_1 = nt_2$. Како је

$$(ab)^t = a^t b^t = a^{mt_1} b^{nt_2} = (a^m)^{t_1} (b^n)^{t_2} = e^{t_1} e^{t_2} = e,$$

то добијамо $s \mid t$.

С обзиром да је $s = \omega(ab)$,

$$e = (ab)^s = a^s b^s.$$

Добијамо да је $a^s = (b^s)^{-1}$. Но, $a^s \in \langle a \rangle$, а $(b^s)^{-1} \in \langle b \rangle$ те смо добили елемент из пресека $\langle a \rangle \cap \langle b \rangle$. Како је овај пресек тривијалан, мора бити $a^s = e$ и $(b^s)^{-1} = e$, тј. $b^s = e$. Но, с обзиром на то да је $m = \omega(a)$ и $n = \omega(b)$, следи да $m \mid s$ и $n \mid s$. Имајући у виду да је $t = \text{NZS}(m, n)$, добијамо да $t \mid s$. Закључујемо да је $s = t$. □

Из овог резултата можемо добити две последице.

Последица 25 Ако су σ и τ дисјунктни циклуси из $\mathbb{S}_n$, онда је $\omega(\sigma\tau) = \text{NZS}(\omega(\tau), \omega(\sigma))$.

Доказ. Да бисмо применили претходни став, довољно је показати да је $\langle \tau \rangle \cap \langle \sigma \rangle = \{(1)\}$. Претпоставимо да је $\pi \in \langle \tau \rangle \cap \langle \sigma \rangle$. Нека је $\sigma = (a_1 \dots a_k)$, а $\tau = (b_1 \dots b_l)$. Нека је $i \in \{1, \dots, n\}$ произвољан елемент. Ако $i \notin \{a_1, \dots, a_k\}$, с обзиром да је $\pi = \sigma^s$, за неко s, мора бити $\pi(i) = i$. Ако пак $i \in \{a_1, \dots, a_k\}$, онда $i \notin \{b_1, \dots, b_l\}$, те с обзиром да је $\pi = \tau^t$, за неко t, мора бити $\pi(i) = i$. Закључујемо да је π идентична пермутација, те је пресек тривијалан. □

Следећи резултат је генерализација претходног.

Последица 26 Ако је $\pi = \sigma_1 \cdots \sigma_k$ представљање пермутације π у облику производа дисјункних циклуса, онда је $\omega(\pi) = \text{NZS}(\omega(\sigma_1), \dots, \omega(\sigma_k))$.

Искористимо управо доказано на једном примеру.

Пример 27 а) Испитати да ли у $\mathbb{S}_7$ постоји елемент реда 12.

б) Испитати да ли у $\mathbb{S}_7$ постоји елемент реда 8.

а) Елемент $(1234)(567)$ је на основу претходних резултата реда 12.
б) Питање се своди на следеће. Да ли број 8 може бити најмањи заједнички садржалац бројева мањих од њега? Да то није могуће, може се установити једноставном анализом. Остављамо читаоцима да се у то увере.

Ми смо се до сада бавили цикличним, диедарским и групама пермутација. Да ли се можда неке од ових група подударају? Није тешко видети да су групе $\mathbb{S}_2$ и $\mathbb{A}_3$ цикличне групе (реда 2 односно 3). Много је занимљивија следећа чињеница:

$$\mathbb{D}_3 \cong \mathbb{S}_3.$$

Наиме, група $\mathbb{D}_3$ је група симетрија једнакостраничног троугла. Означимо темена тог троугла бројевима 1, 2 и 3. Свака симетрија троугла индукује једну пермутацију скупа свих темена, а тиме и скупа $\{1, 2, 3\}$. Није тешко уверити се која пермутација одговара којој симетрији троугла. Препоручујемо читаоцима да нацртају цртеж и сами одреде наведене симетрије. Такође за вежбу остављамо да читаоци сами покажу да ниједна од група $\mathbb{S}_n$, $\mathbb{D}_n$, за $n \geq 3$, није циклична.

Размотримо два занимљива примера из геометрије.

Пример 28 Група ротационих симетрија правилног тетраедра изоморфна је групи $\mathbb{A}_4$.

И овде је добро темена тетраедра нумерисати бројевима од 1 до 4. Свака ротациона симетрија индукује пермутацију скупа темена. Тако добијамо функцију из групе симетрија тетраедра у групу $\mathbb{A}_4$ (уверите се да добијамо само парне пермутације). Но, та функција не само да је бијекција, него је и изоморфизам, пошто је у оба случаја операција у групи заправо композиција пресликавања. ♣

Пример 29 Група ротационих симетрија коцке изоморфна је групи $\mathbb{S}_4$.

Размотримо најпре колико има ротационих симетрија коцке. Како коцка има 6 страна, то за сваки пар страна постоје по три нетривијалне ротације коцке око оса које пролазе кроз центре наспрамних страна. Ротације су за $\pi/2$, π и $3\pi/2$. Тако добијамо 9 ротација.

Коцка има и 4 дијагонале и око сваке дијагонале постоје две нетривијалне ротације — за углове од $2\pi/3$ и $4\pi/3$. Дакле, добијамо још 8 ротација.

Коцка има и 12 ивица. Постоји 6 ротација за π око оса које пролазе кроз средишта наспрамних ивица коцке.

Укупно смо добили $9+8+6+1 = 24$ ротације (додали смо и идентичну трансформацију).

Свака од ротација пермутује дијагонале коцке. Тако се свака ротација може видети и као пермутација скупа од 4 елемента. Све оне

су различите, а има их 24 колико и елемената групе $\mathbb{S}_4$. С обзиром да су у оба случаја групне операције композиција функција добијамо да је тражена група симетрија изоморфна групи $\mathbb{S}_4$. Препоручујемо читаоцима да детаљније проуче овај пример и провере које ротације одговарају којим елементима из $\mathbb{S}_4$. ♣

За крај ове лекције докажимо једну једноставну, али веома важну теорему, која показује зашто групе пермутација имају значајно место у теорији група.

Теорема 30 (Кејлијева теорема) Свака група G изоморфна је некој подгрупи групе $\mathbb{S}_G$.

Доказ. Ако је $g \in G$, са $L_g: G \to G$ означимо бијекцију дефинисану са:

$$L_g(x) := g \cdot x.$$

Јасно је да је L_g бијекција пошто је $L_g \circ L_{g^{-1}} = \mathrm{id}_G (= L_e)$. Дакле, $(L_g)^{-1} = L_{g^{-1}}$. Осим тога:

$$L_g \circ L_h = L_{g \cdot h}.$$

Дакле, видимо да је $G' = \{L_g : g \in G\}$ једна подгрупа групе $\mathbb{S}_G$.

Функција $f: G \to G'$ дефинисана са $f(g) = L_g$ остварује изоморфизам између G и G'. □

У случају да је група коначна добијамо следећу последицу.

Последица 31 Свака коначна група реда n изоморфна је некој подгрупи групе $\mathbb{S}_n$.

Директан производ група; Лагранжова теорема

Један од начина на који од већ постојећих група можемо формирати нове групе је *директан производ група*.

Дефиниција 32 Нека су $(G_1, *_1), (G_2, *_2), \ldots, (G_1, *_n)$ групе. Дефинишемо директан производ $(P, *)$ ових група са:

- $P := G_1 \times G_2 \times \cdots G_n$;
- $(g_1, g_2, \ldots, g_n) * (g_1', g_2', \ldots, g_n') := (g_1 *_1 g_1', g_2 *_2 g_2', \ldots, g_n *_n g_n')$.

Није тешко проверити да је $(P, *)$ заиста група. Наиме, асоцијативност се лако проверава, док је неутрални елемент $e \in P$ дат са:

$$e = (e_1, e_2, \ldots, e_n),$$

где је e_i неутрални елемент у групи G_i. Такође је јасно шта је инверзни елемент:

$$(x_1, x_2, \ldots, x_n)^{-1} = (x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}).$$

Погледајмо за почетак неке једноставне примере.

Пример 33 Група $\mathbb{Z}_2 \times \mathbb{Z}_3$ је циклична група.

Приметимо најпре да је скуп носач структуре $\mathbb{Z}_2 \times \mathbb{Z}_3$, скуп

$$\{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

Да бисмо показали да је група циклична, морамо наћи елемент, који је генерише, тј. елемент реда 6. Није тешко уверити се да је један такав елемент, елемент $(1,1)$:

$$\begin{aligned}
(1,1) + (1,1) &= (1 +_2 1, 1 +_3 1) = (0,2);\\
(1,1) + (1,1) + (1,1) &= (1 +_2 0, 1 +_3 2) = (1,0);\\
(1,1) + (1,1) + (1,1) + (1,1) &= (1 +_2 1, 1 +_3 0) = (0,1);\\
(1,1) + (1,1) + (1,1) + (1,1) + (1,1) &= (1 +_2 0, 1 +_3 1) = (1,2);\\
(1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) &= (1 +_2 1, 1 +_3 2) = (0,0).
\end{aligned}$$

Остављамо читаоцима да провере да ли је још неки елемент генератор ове групе. ♣

Пример 34 Група $\mathbb{Z}_2 \times \mathbb{Z}_2$ није циклична група.

Скуп носач је скуп $\{(0,0), (0,1), (1,0), (1,1)\}$. Но, није тешко уверити се да је сваки елемент у овом скупу, осим неутрала, реда 2:

$$\begin{aligned}
(0,1) + (0,1) &= (0 +_2 0, 1 +_2 1) = (0,0);\\
(1,0) + (1,0) &= (1 +_2 1, 0 +_2 0) = (0,0);\\
(1,1) + (1,1) &= (1 +_2 1, 1 +_2 1) = (0,0).
\end{aligned}$$

♣

Природно се поставља питање: за које $m, n \geq 2$ је група $\mathbb{Z}_m \times \mathbb{Z}_n$ циклична група? Одговор на ово питање даје следећи став.

Став 35 Група $\mathbb{Z}_m \times \mathbb{Z}_n$ је циклична ако и само ако је $\mathrm{NZD}(m,n) = 1$.

Доказ.
$\Longrightarrow$: Претпоставимо да је $\mathrm{NZD}(m,n) = d > 1$. Покажимо да тада група $\mathbb{Z}_m \times \mathbb{Z}_n$ не може бити циклична. Нека је $r = \frac{mn}{d} < mn$. Покажимо да је

$$\underbrace{x + \cdots + x}_{r} = 0,$$

за све $x \in \mathbb{Z}_m \times \mathbb{Z}_n$. Нека је $x = (s,t)$, произвољан елемент групе $\mathbb{Z}_m \times \mathbb{Z}_n$. Дакле, знамо да је $s \in \{0,1,\ldots,m-1\}$ и $t \in \{0,1,\ldots,n-1\}$ и да важи:

$$\underbrace{s +_m \cdots +_m s}_{m} = 0, \quad \underbrace{t +_n \cdots +_n t}_{n} = 0.$$

Но, тада је

$$\underbrace{s +_m \cdots +_m s}_{r} = \underbrace{\underbrace{(s +_m \cdots +_m s)}_{m} +_m \cdots +_m \underbrace{(s +_m \cdots +_m s)}_{m}}_{\frac{n}{d}} = \underbrace{0 +_m \cdots +_m 0}_{\frac{n}{d}} = 0,$$

као и

$$\underbrace{t +_n \cdots +_n t}_{r} = \underbrace{\underbrace{(t +_n \cdots +_n t)}_{n} +_n \cdots +_n \underbrace{(t +_n \cdots +_n t)}_{n}}_{\frac{m}{d}} = \underbrace{0 +_n \cdots +_n 0}_{\frac{m}{d}} = 0.$$

Одавде следи да је

$$\underbrace{(s,t) + \cdots + (s,t)}_{r} = 0,$$

те је ред сваког елемента у групи $\mathbb{Z}_m \times \mathbb{Z}_n$ највише r, дакле мањи од mn, те група не може бити циклична.
$\Longleftarrow$: Претпоставимо да је $\mathrm{NZD}(m,n) = 1$. Докажимо да је елемент $(1,1)$ генератор групе $\mathbb{Z}_m \times \mathbb{Z}_n$, тј. да је ред тог елемента једнак mn. Означимо са r ред елемента $(1,1)$. Дакле,

$$\underbrace{(1,1) + \cdots + (1,1)}_{r} = (0,0).$$

То значи да је

$$\underbrace{1 +_m \cdots +_m 1}_{r} = 0$$

у групи $\mathbb{Z}_m$, из чега следи да $m \mid r$, као и

$$\underbrace{1 +_n \cdots +_n 1}_{r} = 0$$

у групи $\mathbb{Z}_n$, из чега следи да $n \mid r$. Дакле, $\mathrm{NZS}(m,n) \mid r$. Но, како су m и n узајамно прости, то је $\mathrm{NZS}(m,n) = mn$ и закључујемо да $mn \mid r$. Дакле, ред елемента $(1,1)$ у групи $\mathbb{Z}_m \times \mathbb{Z}_n$ је бар mn те закључујемо да је та група циклична. □

Напомена. У случају да је група G комутативна, тј. да за све $x, y \in G$ важи: $xy = yx$, уобичајено је за ознаку операције у групи користити

ознаку $+$. У том случају ознака mx, где је $m \in \mathbb{Z}$ одговара ознаци x^m. Нпр.

$$6x = \underbrace{x + \cdots + x}_{6}.$$

Како је свака циклична група реда n изоморфна групи $\mathbb{Z}_n$, то закључујемо да је директан производ цикличне групе реда m и цикличне групе реда n циклична група (реда mn) ако и само ако су m и n узајамно прости. Приметимо да се у овом тврђењу имплицитно „крије" следећи резултат: ако је $G \cong G'$ и $H \cong H'$, онда је $G \times H \cong G' \times H'$. Размислите како бисте ово доказали.

Индукцијом није тешко показати да важи следећи резултат. Ако су $m_1, m_2, \ldots, m_n$ пар по пар узајамно прости, онда имамо изоморфизам група

$$\mathbb{Z}_{m_1 m_2 \cdots m_n} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}.$$

Осим што се конструкција директног производа може искористити за добијање нових група од старих, она се може употребити и за испитивање структуре неке дате групе. Наиме, корисно је знати да је нека група изоморфна директном производу других група. У ту сврху користан је следећи став.

Став 36 Нека је G група, а H и K подгрупе групе G за које важи:

1. $G = H \cdot K$;
2. за све $x \in H$ и све $y \in K$: $xy = yx$;
3. $H \cap K = \{e\}$.

Тада је $G \cong H \times K$.

Доказ. Напоменимо најпре да је $H \cdot K = \{h \cdot k : h \in H, k \in K\}$. Дефинишемо функцију $f : H \times K \to G$ са:

$$f(h, k) := hk.$$

Докажимо да је f изоморфизам група. Пре свега, како је $G = H \cdot K$, јасно је да је f „на". Да бисмо доказали да је хомоморфизам, морамо проверити да важи следеће:

$$\text{за све } h, h' \in H \text{ и све } k, k' \in K : f((h, k) \cdot (h', k')) = f(h, k) \cdot f(h', k'),$$

тј. да за све $h, h' \in H, k, k' \in K$:

$$hh'kk' = hkh'k'.$$

Но, како по претпоставци елементи из H и елементи из K међусобно комутирају, то наведена једнакост јесте испуњена.

Остаје да проверимо да је f „1–1”. Претпоставимо да је

$$f(h,k) = f(h',k').$$

То значи да је

$$hk = h'k',$$

односно

$$(h')^{-1}h = k'k^{-1}.$$

Но, како $(h')^{-1}h$ припада подгрупи H, а $k'k^{-1}$ подгрупи K, то смо добили елемент из $H \cap K$, а та подгрупа је тривијална. Закључујемо да мора бити $(h')^{-1}h = e$ и $k'k^{-1} = e$, те следи да је $h = h'$ и $k = k'$, тј. $(h,k) = (h',k')$. □

Ради илустрације примене ове теореме, урадимо два примера.

Пример 37 $\mathbb{D}_6 \cong \mathbb{D}_3 \times \mathbb{Z}_2$.

Дакле, у групи $\mathbb{D}_6$ треба наћи једну подгрупу изоморфну са $\mathbb{D}_3$ и једну изоморфну са $\mathbb{Z}_2$ чији је пресек тривијалан, а елементи међусобно комутирају. Група $\mathbb{D}_6$ је група симетрија правилног шестоугла, док је групе $\mathbb{D}_3$ група симетрија једнакостраничног троугла. Где се у правилном шестоуглу „крије” једнакостранични троугао? Није тешко видети да, ако су темена правилног шестоугла A, B, C, D, E, F, дијагонале AC, CE, EA образују једнакостранични троугао. Ротација шестоугла за угао $2\pi/3$, тј. ротација ρ^2, јесте симетрија тог троугла. Ако за σ узмемо осну рефлексију око праве која садржи дијагоналу BE, онда се лако можемо уверити да је подгрупа $H = \{\varepsilon, \rho^2, \rho^4, \sigma, \sigma\rho^2, \sigma\rho^4\}$, изоморфна групи $\mathbb{D}_3$. Ако за групу K узмемо групу генерисану елементом ρ^3, тј. ако је $K = \{\varepsilon, \rho^3\}$, то лако проверавамо да је $H \cdot K = \mathbb{D}_6$. Осим тога, елемент ρ^3 комутира са свим елементима из H ($\sigma\rho^3 = \rho^{-3}\sigma = \rho^3\sigma$, па заправо ρ^3 комутира са свим елементима из $\mathbb{D}_6$). Како је $H \cap K = \{\varepsilon\}$, на основу претходног става закључујемо да је $\mathbb{D}_6 \cong H \times K$, тј. $\mathbb{D}_6 \cong \mathbb{D}_3 \times \mathbb{Z}_2$. ♣

Пример 38 Ако је G коначна група чији је сваки елемент, сем неутрала, реда 2, онда је G изоморфна директном производу цикличних група реда 2.

Докажимо најпре да је група у којој је сваки елемент реда 2 комутативна. Нека су a и b произвољни елементи из G. По претпоставци је $a^2 = e$, $b^2 = e$, $(ab)^2 = e$. Одавде следи да је

$$(ab)^2 = a^2b^2,$$

тј.

$$abab = aabb,$$

што, после скраћивања, даје

$$ab = ba.$$

Нека је $x_1 \neq e$ произвољан елемент групе G, различит од неутрала. Посматрајмо подгрупу H_1 генерисану тим елементом. Она је реда 2 пошто је елемент реда x_1 реда 2. Уколико је $H_1 = G$, доказ је завршен. У супротном, изаберимо елемент $x_2 \in G \setminus H_1$ и нека је $K_2 = \langle x_2 \rangle$. Тада је $H_2 = H_1 \cdot K_2 = \{e, x_1, x_2, x_1x_2\}$ једна подгрупа групе G (проверите!). Подгрупе H_1 и K_2 испуњавају услове претходног става (зашто?), те добијамо да је $H_2 \cong H_1 \times K_2$. Уколико је $H_2 = G$, доказ је завршен. У супротном, бирамо елемент $x_3 \in G \setminus H_2$ и посматрамо подгрупу $K_3 = \langle x_3 \rangle$. Као и у претходном случају $H_3 = H_2 \cdot K_3$ је подгрупа групе G и $H_3 \cong H_2 \times K_3 \cong H_1 \times K_2 \times K_3$. Овакав поступак мора се завршити пошто је група G коначна, а $|H_k| = 2^k$. Стога добијамо да је за неко n испуњено $G \cong H_1 \times K_2 \times \cdots \times K_n$, а сви ови фактори су цикличне групе реда 2. ♣

Подсетимо се да смо увели појам реда групе и реда елемента. У случају цикличне групе, ред саме групе једнак је реду елемента који генерише ту групу. Природно је поставити питање о вези између реда елемента и реда коначне групе и у случају да група није циклична. Још општије, каква је веза између реда коначне групе и реда неке њене подгрупе? Испоставља се да је одговор једноставан и сада ћемо се тиме позабавити.

Дефиниција 39 Ако је $H \leq G$ и $x \in G$, скуп

$$xH = \{x \cdot h : h \in H\},$$

назива се леви косет подгрупе H у групи G. Аналогно, скуп

$$Hx = \{h \cdot x : h \in H\},$$

назива се десни косет.

Како $e \in H$, косет xH (Hx) садржи елемент x. У општем случају $xH \neq Hx$. Нпр. ако је $G = \mathbb{D}_3$ и $H = \{\varepsilon, \sigma\}$, онда је

$$H\rho = \{\rho, \sigma\rho\} \neq \{\rho, \rho\sigma\} = \rho H,$$

пошто је $\rho\sigma = \sigma\rho^2$. Скуп свих левих косета подгрупе H у G означаваћемо са G/H, а свих десних косета са $H\backslash G$. Као што смо видели, леви косет, који садржи елемент x, не мора бити једнак десном косету који садржи тај елемент, па је у општем случају $G/H \neq H\backslash G$. У наредним лекцијама видећемо када су ови скупови једнаки, али то је друга прича. За сада само можемо да закључимо да постоји бијекција између њих која левом косету xH придружује десни косет Hx.

Став 40 Важи следеће:

1. $xH = yH$ ако и само ако је $x^{-1}y \in H$;

2. ако је $xH \neq yH$, онда је $xH \cap yH = \emptyset$.

Доказ.
1. $\Longrightarrow$: Претпоставимо да је $xH = yH$. То посебно значи да $y \in xH$, тј. постоји $h \in H$ за који је $y = xh$. Но, тада је $h = x^{-1}y$, па закључујемо да $x^{-1}y \in H$.

$\Longleftarrow$: Нека $x^{-1}y \in H$. Претпоставимо да $z \in xH$. Дакле, $z = xh$, за неко $h \in H$. Тада је $z = x(x^{-1}y)(x^{-1}y)^{-1}h = y((x^{-1}y)^{-1}h)$, но, како је H подгрупа од G и $x^{-1}y \in H$, то и $(x^{-1}y)^{-1}h \in H$, па закључујемо да $z \in yH$. Обратно, ако $z \in yH$, онда постоји $h' \in H$, такав да је $z = yh'$. Тада је $z = x((x^{-1}y)h')$, а како је $x^{-1}y \in H$ и како је H подгрупа од G, то $z \in xH$. Закључујемо да је $xH = yH$ уколико $x^{-1}y \in H$.

2. Претпоставимо да је $xH \cap yH \neq \emptyset$. То значи да за неке $h, h' \in H$ важи: $xh = yh'$. Одавде следи да је $x^{-1}y = h(h')^{-1}$, а како је $H \leq G$, то $h(h')^{-1} \in H$. На основу претходно доказаног, следи да је $xH = yH$. □

Дакле, различити леви косети ма које подгрупе H су дисјунктни. Како сваки елемент x лежи у косету xH, то закључујемо да важи следећи став.

Став 41 Нека је G група и $H \leq G$. Тада је G дисјунктна унија различитих левих косета подгрупе H.

Дефиниција 42 Уколико је скуп левих косета G/H бесконачан, кажемо да је подгрупа H бесконачног индекса у групи G. Уколико је тај скуп коначан, онда се индекс подгрупе H у групи G, у ознаци $[G : H]$, дефинише као број елемената у G/H, тј. $[G : H]$ је број различитих левих косета подгрупе H у групи G.

Напомена. Како постоји бијекција између G/H и $H\backslash G$, то је $[G : H]$ такође и број различитих десних косета H у G. Осим тога, бесконачна група може садржати подгрупе коначног индекса. На пример, подгрупа од $\mathbb{Z}$ генерисана елементом 3 је индекса 3 (проверити ово).

Теорема 43 (Лагранжова теорема) Нека је G коначна група и $H \leq G$. Тада је

$$|G| = |H| \cdot [G : H].$$

Посебно, ред подгрупе H дели ред групе G.

Доказ. Како је група G коначна, то је очигледно G коначна унија левих косета подгрупе H, тј. за неке $x_1, \ldots, x_k \in G$ важи:

$$G = x_1H \sqcup x_2H \sqcup \cdots \sqcup x_kH,$$

при чему је $k = [G : H]$. Но, $|xH| = |yH|$ за све $x, y \in G$. Наиме, функција $f : xH \to yH$ дефинисана са: $f(xh) = yh$ задаје бијекцију између ова два скупа (проверите ово). Добијамо да је $|G| = |H| \cdot k = |H| \cdot [G : H]$. □

Наведимо неке последице Лагранжове теореме.

Последица 44 Ред сваког елемента коначне групе дели ред те групе.

Доказ. Нека је G коначна група и $x \in G$. Јасно је да ред елемента x мора бити коначан. Осим тога, $\omega(x) = |\langle x \rangle|$, а према Лагранжовој теореми $|\langle x \rangle| \mid |G|$. Дакле, $\omega(x) \mid |G|$. □

Последица 45 Свака група простог реда је циклична.

Доказ. Нека је $|G| = p$, где је p прост број. Ако је x било који елемент из G различит од неутрала, онда је $\omega(x) \neq 1$ и $\omega(x) \mid p$. Закључујемо да је $\omega(x) = p$, те је $\langle x \rangle = G$. □

Последица 46 Ако је G коначна група и $x \in G$, онда је $x^{|G|} = e$.

Доказ. Присетимо се да је $x^n = e$ ако и само ако $\omega(x) \mid n$. Како $\omega(x) \mid |G|$, резултат следи. □

У скупу $Z_n = \{0, 1, \ldots, n-1\}$, где је $n \geq 2$ можемо увести операцију $\cdot_n$ (множење по модулу n). Наравно, у односу на ову операцију Z_n не чини групу (зашто?). Посматрајмо стога следећи скуп.

$$\Phi(n) := \{k : 1 \leq k < n, \mathrm{NZD}(k, n) = 1\}.$$

Важи следећи став.

Став 47 За све $n \geq 2$, $(\Phi(n), \cdot_n)$ је комутативна група.

Доказ. Најпре треба проверити да ли множење по модулу n заиста задаје бинарну операцију на скупу $\Phi(n)$, тј. да ли је испуњено следеће:

$$\text{ако } x, y \in \Phi(n) \text{ онда } x \cdot_n y \in \Phi(n).$$

Уколико је $\mathrm{NZD}(x, n) = 1 = \mathrm{NZD}(y, n)$, онда је и $\mathrm{NZD}(x \cdot y, n) = 1$. Наиме, добро нам је познато следеће:

$$\mathrm{NZD}(a, b) = 1 \textbf{ акко } \text{постоје } p, q \in \mathbb{Z} \text{ тако да је } ap + bq = 1.$$

Дакле, постоје $p, q \in \mathbb{Z}$ за које је $xp + nq = 1$, као и $p', q' \in \mathbb{Z}$ за које је $yp' + nq' = 1$. Множењем ове две релације, добијамо да је

$$xy(pp') + n(qyp' + xpq' + nqq') = 1,$$

те мора бити $\mathrm{NZD}(x \cdot y, n) = 1$. С обзиром да је

$$x \cdot y \equiv x \cdot_n y \pmod{n},$$

то је и $\mathrm{NZD}(x \cdot_n y, n) = 1$.

Познато нам је да је операција $\cdot_n$ асоцијативна и комутативна. Осим тога, $1 \in \Phi(n)$, па постоји и неутрални елемент за ову операцију. Но, сваки елемент из $\Phi(n)$ заиста има инверз. Наиме, ако $x \in \Phi(n)$, онда постоје $p, q \in \mathbb{Z}$ за које је $xp + yq = 1$. Ако са $\bar{p}$ означимо елемент из Z_n,

који је конгруентан елементу p по модулу n, онда је $\bar{p} \in \Phi(n)$ и осим тога је $x \cdot_n \bar{p} = 1$. □

Ред групе $\Phi(n)$ означавамо са $\varphi(n)$. Ова функција φ зове се Ојлерова функција.

Последица 48 (Ојлерова теорема) Нека је $n \geq 2$ и x цео број, узајамно прост са n, онда је

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Доказ. Како је x узајамно прост са n, то је x конгруентан по модулу n неком броју $\bar{x} \in \Phi(n)$. Но, $|\Phi(n)| = \varphi(n)$ и на основу Последице **??** знамо да у групи $\Phi(n)$ важи једнакост $\bar{x}^{\varphi(n)} = 1$. То заправо значи да је $x^{\varphi(n)}$ конгруентно са 1 по модулу n. □

У случају да је p прост број, очигледно је да је $\varphi(p) = p - 1$. Стога добијамо још једну последицу Лагранжове теореме.

Последица 49 (Мала Фермаова теорема) Ако је p прост број, који не дели цео број x, онда је

$$x^{p-1} \equiv 1 \pmod{p}.$$

Пример 50 Нека је p прост и $n \geq 2$. Тада $n \mid \varphi(p^n - 1)$.

Како се у формулацији примера појављује $\varphi(p^n - 1)$, то је очигледно да треба да искористимо групу $\Phi(p^n - 1)$ (чији је ред $\varphi(p^n - 1)$). Пошто је потребно да докажемо да $n \mid \varphi(p^n - 1)$, то је природно да у групи $\Phi(p^n - 1)$ потражимо елемент реда n. Но, није га тешко наћи — то је заправо елемент p. Наиме, $\mathrm{NZD}(p, p^n - 1) = 1$, те $p \in \Phi(p^n - 1)$. Осим тога, елементи p^k за $1 \leq k \leq n - 1$ очигледно нису једнаки 1 у групи $\Phi(p^n - 1)$, док је

$$p^n = 1 + (p^n - 1) \equiv_{p^n - 1} 1.$$

Стога је заиста ред елемента p једнак n, а како ред елемента дели ред групе, добијамо тражени резултат. ♣

Како израчунати $\varphi(n)$ за произвољно $n \geq 2$? За функцију φ важи следеће:

1. уколико су m и n узајамно прости, онда је $\varphi(mn) = \varphi(m)\varphi(n)$;
2. за сваки прост број p и $m \geq 1$: $\varphi(p^m) = p^m - p^{m-1}$.

Прву особину доказаћемо када се будемо бавили комутативним прстенима са јединицом, док се друга лако доказује. Наиме, $x \in Z_{p^m} \setminus \{0\}$ није у $\Phi(p^m)$ ако и само ако $p \mid x$. Дакле,

$$x \notin \Phi(p^m) \textbf{ акко } x \in \{p, 2p, \ldots, (p^{m-1} - 1)p\}.$$

Према томе,

$$\begin{aligned}\varphi(p^m) &= |\Phi(p^m)| \\ &= |Z_{p^m} \setminus \{0\}| - |\{p, 2p, \ldots, (p^{m-1}-1)p\}| \\ &= (p^m - 1) - (p^{m-1} - 1) \\ &= p^m - p^{m-1}.\end{aligned}$$

Коришћењем ова два својства, добијамо да важи следећи резултат. Ако је $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ факторизација броја n на просте факторе, онда је

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}) \\ &= \varphi(p_1^{m_1})\varphi(p_2^{m_2}) \cdots \varphi(p_k^{m_k}) \\ &= p_1^{m_1-1}(p_1-1)p_2^{m_2-1}(p_2-1)\cdots p_k^{m_k-1}(p_k-1) \\ &= p_1^{m_1}\left(1-\frac{1}{p_1}\right)p_2^{m_2}\left(1-\frac{1}{p_2}\right)\cdots p_k^{m_k}\left(1-\frac{1}{p_k}\right) \\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

Групе малог реда; класе конјугације

Лагранжова теорема нам показује да, на пример, група реда 20 не може да има подгрупу реда 12 и слично. Она нам не говори ништа о томе да ли, на пример, група реда 20 има подгрупу реда 10 (постојање такве подгрупе не би било у супротности са Лагранжовом теоремом). Оваква питања су знатно сложенија и ми се њима нећемо сада бавити. Само ћемо навести једну теорему (за сада без доказа), која говори о постојању подгрупа одређеног реда и навести неке њене последице у облику примера.

Теорема 51 (Кошијева теорема) Ако је G коначна група и p прост број такав да $p \mid |G|$, онда у G постоји елемент реда p.

Дакле, уколико је p прост број, који дели ред групе G, у G постоји елемент реда p, а самим тим и подгрупа реда p.

Пример 52 Свака група реда 6 изоморфна је или групи $\mathbb{Z}_6$ или групи $\mathbb{D}_3$.

Нека је $|G| = 6$. Уколико у G постоји елемент реда 6, онда је $G \cong \mathbb{Z}_6$. Претпоставимо стога да у G не постоји елемент реда 6. На основу Кошијеве теореме у G постоји елемент x реда 3 и елемент y реда 2 (добра је вежба доказати ово без коришћења Кошијеве теореме – покушајте!). Како је $3 = \omega(x) = \omega(x^2)$ (зашто?), то $y \notin \langle x \rangle$. Стога је

$$G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, x^2, y, yx, yx^2\}.$$

Елемент xy је у G и једнак је неком од наведених елемената. Није тешко уверити се (уверите се!) да су једине могућности:

1. $xy = yx$;
2. $xy = yx^2$.

Но, ако је $xy = yx$, добијамо да је

$$G \cong \langle y \rangle \times \langle x \rangle \cong \mathbb{Z}_6$$

(зашто?), што противречи претпоставци да у G нема елемената реда 6. Преостаје могућност $xy = yx^2$ и у том случају је $G \cong \mathbb{D}_3$ (при изоморфизму који x слика у ρ, а y у σ). ♣

Завршићемо ову лекцију описом група реда 8. Да бисмо могли да је извршимо, биће нам потребан још један пример групе.

Добро нам је познато рачунање са комплексним бројевима. Сваки комплексан број се може написати у облику $a + bi$, где су a и b реални бројеви, а i је имагинарна јединица, тј. за i важи следеће: $i^2 = -1$. Хамилтон је у математику увео кватернионе. Сваки кватернион може се написати у облику $a + bi + cj + dk$, где су a, b, c, d реални бројеви, а i, j, k имагинарне јединице за које још важи: $ij = k = -ji, jk = i = -kj, ki = j = -ik$. Као што се може видети, множење кватерниона није комутативно, но многа друга својства, која важе за комплексне бројеве важе и за кватернионе. И поред занимљивости кватерниона, ми се нећемо њима детаљно бавити. Но, означимо са Q_8 следећи скуп:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Није тешко уверити се да је $(Q_8, \cdot)$ група. Зовемо је кватернионска група. Наведимо таблицу ове групе.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Приметимо да је Q_8 генерисана елементима i и j и да за ове елементе важи: $i^2 = j^2$ и $jij^{-1} = i^{-1}$.

Пример 53 Свака група реда 8 изоморфна је тачно једној од група:

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{D}_4, \quad Q_8.$$

Нека је G група реда 8. Уколико у G постоји елемент реда 8, онда је $G \cong \mathbb{Z}_8$. Уколико је пак у G сваки елемент реда 2, према ранијем резултату следи да је $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Претпоставимо у даљем да у G постоји елемент реда 4 и да не постоји елемент реда 8.

Нека је x реда 4 и нека $y \notin \langle x \rangle$. Тада је

$$G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, x^2, x^3, y, yx, yx^2, yx^3\}.$$

Одредимо који од ових елемената може бити једнак елементу xy. Пре свега, како $y \notin \langle x \rangle$ и како је $x \neq e$, то $xy \notin \{e, x, x^2, x^3, y\}$. Уколико је пак $xy = yx^2$, добијамо да је $x = yx^2y^{-1}$ из чега следи да је $x^2 = yx^4y^{-1} = yey^{-1} = e$, па би x био реда 2, што није. Закључујемо да $xy \in \{yx, yx^3\}$.

Одредимо још колико је y^2. Пре свега, како $y \notin \langle x \rangle$, то $y^2 \notin y\langle x \rangle$. Осим тога, како је $\omega(x) = \omega(x^3) = 4$, а у G нема елемената реда 8 то y^2 не може бити ни x ни x^3 (тада би y био реда 8). Дакле, $y^2 \in \{e, x^2\}$.

Добили смо 4 случаја

1. $xy = yx$, $y^2 = e$;
2. $xy = yx$, $y^2 = x^2$;
3. $xy = yx^3$, $y^2 = e$;
4. $xy = yx^3$, $y^2 = x^2$.

Размотримо сваки посебно.

1. У овом случају је група G комутативна и функција $f\colon \mathbb{Z}_2 \times \mathbb{Z}_4 \to G$ дефинисана са $f(r, s) = y^r x^s$ је изоморфизам. Јасно је да је f бијекција. Само треба проверити слагање са операцијама.

$$f(r +_2 r', s +_4 s') = y^{r+_2 r'} x^{s+_4 s'}.$$

Како је y реда 2 и x реда 4, то је $y^{r+_2 r'} = y^r y^{r'}$ и $x^{s+_4 s'} = x^s x^{s'}$. Дакле,

$$f(r +_2 r', s +_4 s') = y^r y^{r'} x^s x^{s'}.$$

Како је $xy = yx$, то је

$$y^r y^{r'} x^s x^{s'} = y^r x^s y^{r'} x^{s'} = f(r, s) f(r', s').$$

Дакле, заиста је

$$f(r +_2 r', s +_4 s') = f(r, s) f(r', s').$$

2. У овом случају је такође група G комутативна. Приметимо да је сада елемент y реда 4, но елемент $y^3 x$ је реда 2:

$$(y^3 x)^2 = y^6 x^2 = x^6 x^2 = x^8 = e.$$

Стога је изоморфизам $f\colon \mathbb{Z}_2 \times \mathbb{Z}_4 \to G$ задат са: $f(r,s) = (y^3x)^r x^s$. Проверите детаље!

3. У овом случају, ситуација је јасна. Изоморфизам $f\colon \mathbb{D}_4 \to G$ задат је са: $f(\sigma) = y$, $f(\rho) = x$.

4. И у овом случају није тешко видети како функција $f\colon Q_8 \to G$ задата са: $f(i) = x$, $f(j) = y$ задаје изоморфизам (важно је приметити да је $ij = k = ji^3$ и $i^2 = j^2$). ♣

Уведимо сада један веома важан појам.

Дефиниција 54 Елемент y је конјугован елементу x (елемент y је конјугат елемента x) у групи G уколико постоји $g \in G$ тако да је

$$y = gxg^{-1}.$$

Јасно је да је на овај начин дефинисана једна релација еквиваленције на скупу G. Наиме, сваки елемент x је конјугован сам себи пошто је $x = exe^{-1}$. Уколико је y конјугован елементу x, тј. постоји $g \in G$ тако да је $y = gxg^{-1}$, онда је и x конјугован y, јер је $x = g^{-1}y(g^{-1})^{-1}$. Ако је y конјугован елементу x ($y = gxg^{-1}$ за неко $g \in G$), а z конјугован елементу y ($z = hyh^{-1}$), онда је и z конјугован елементу x: $z = (hg)x(hg)^{-1}$.

Класу еквиваленције при овој релацији зовемо класа конјугације (или класа конјугованости).

Пример 55 Одредити класе конјугације у групи $\mathbb{D}_n$.

Разликоваћемо два случаја.

$n = 2l + 1$. Из

$$(\sigma\rho^s)\sigma(\sigma\rho^s)^{-1} = \sigma\rho^s\sigma\sigma\rho^s = \sigma\rho^{2s}$$

и

$$\rho^s\sigma\rho^{-s} = \sigma\rho^{-2s} = \sigma\rho^{2l+1-2s}$$

следи да је једна класа конјугације

$$\{\sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{2l}\}.$$

Из

$$(\sigma\rho^s)\rho^k(\sigma\rho^s)^{-1} = \sigma\rho^s\rho^k\sigma\rho^s = \sigma\sigma\rho^{-s}\rho^{-k}\rho^s = \rho^{-k} = \rho^{2l+1-k},$$

као и из чињенице да је $\rho^s\rho^k\rho^{-s} = \rho^k$, следи да су

$$\{\rho, \rho^{2l}\}, \quad \{\rho^2, \rho^{2l-1}\}, \quad \ldots \quad , \{\rho^l, \rho^{l+1}\}$$

такође класе конјугације. Осим тога, $\{\varepsilon\}$ је једина преостала класа конјугације.

$n = 2l$. Како је

$$(\sigma\rho^s)\sigma(\sigma\rho^s)^{-1} = \sigma\rho^{2s} \quad \text{и} \quad (\sigma\rho^s)\sigma\rho(\sigma\rho^s)^{-1} = \sigma\rho^{2s-1},$$

а

$$\rho^s\sigma\rho^{-s} = \sigma\rho^{-2s} = \sigma\rho^{2l-2s} \quad \text{и} \quad \rho^s\sigma\rho\rho^{-s} = \sigma\rho^{1-2s} = \sigma\rho^{2l+1-2s}$$

то је класа конјугације елемента σ једнака $\{\sigma\rho^{2s} : 0 \leq s \leq l-1\}$, а класа конјугације елемента $\sigma\rho$ је $\{\sigma\rho^{2s+1} : 0 \leq s \leq l-1\}$. Осим тога, како је $\rho^s\rho^k\rho^{-s} = \rho^k$, а

$$(\sigma\rho^s)\rho^k(\sigma\rho^s)^{-1} = \sigma\rho^s\rho^k\sigma\rho^s = \rho^{-k} = \rho^{2l-k},$$

то су двочлане класе конјугације:

$$\{\rho, \rho^{2l-1}\}, \{\rho^2, \rho^{2l-2}\}, \quad \ldots \quad , \{\rho^{l-1}, \rho^{l+1}\},$$

док се једине преостале класе конјугације једночлане:

$$\{\varepsilon\}, \quad \{\rho^l\}.$$

Приметимо на крају да у случају да је n непарно у $\mathbb{D}_n$ постоји само једна једночлана класа конјугације, док их у случају да је n парно има две. ♣

Пример 56 Описати класе конјугације у групи $\mathbb{S}_n$ и одредити их за групе $\mathbb{S}_4$ и $\mathbb{A}_4$.

Приметимо најпре да су ма која два цикла исте дужине конјугована. Наиме, ако су $(a_1a_2\ldots a_k)$ и $(b_1b_2\ldots b_k)$ цикли дужине k из $\mathbb{S}_n$ и ако је π нека пермутација из $\mathbb{S}_n$ за коју је $\pi(a_i) = b_i$ за све $i = \overline{1,k}$, тада је

$$\pi(a_1a_2\ldots a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)\ldots\pi(a_k)) = (b_1b_2\ldots b_k).$$

Општије, важи следеће. Две пермутације σ и ρ из $\mathbb{S}_n$ су конјуговане ако и само ако имају исту циклусну структуру, тј. ако у растављању на производ дисјунктних циклуса у пермутацији σ има исти број циклуса дужине $1, 2, 3, \ldots$ као и у пермутацији ρ. Ово није тешко доказати, али због уштеде времена, доказ нећемо исписивати. Но, резултат би требало да буде очигледан из претходно наведене једнакости.

Позабавимо се сада класама конјугације у групама $\mathbb{S}_4$ и $\mathbb{A}_4$.

У случају групе $\mathbb{S}_4$, можемо користити наведени резултат. Добијамо да су класе конјугације следеће:

$$\{(1234), (1324), (2134), (2314), (3124), (3214)\};$$

$$\{(123), (132), (124), (142), (134), (143), (234), (243)\};$$

$$\{(12), (13), (14), (23), (24), (34)\};$$

$$\{(12)(34), (13)(24), (14)(23)\};$$
$$\{(1)\}.$$

Видимо да постоји само једна једночлана класа конјугације.

У случају групе $\mathbb{A}_4$ морамо пажљивије радити. Нпр. у $\mathbb{A}_4$ циклуси (123) и (132) нису конјуговани. Наиме, ако је π пермутација за коју је

$$\pi(123)\pi^{-1} = (132),$$

она *није* парна пермутација. Наиме, $\pi(4) = 4$, а осим тога мора бити $(\pi(1)\pi(2)\pi(3)) = (132)$, што оставља следеће могућности за π: $\pi = (23)$, или $\pi = (13)$, или $\pi = (12)$. Ниједна од ових пермутација није парна. Дакле, елементи (123) и (132) нису у истој класи конјугације у $\mathbb{A}_4$. Но, ипак није тешко уверити се да су класе конјугације дате са:

$$\{(123), (124), (134), (234)\};$$
$$\{(132), (142), (143), (243)\};$$
$$\{(12)(34), (13)(24), (14)(23)\};$$
$$\{(1)\}.$$

Видимо да и у овом случају постоји само једна једночлана класа конјугације. □

Дефиниција 57 Нека је G група. Центар групе G, у ознаци $Z(G)$ дефинише се као скуп свих елемената из G, који комутирају са свим елементима те групе:

$$Z(G) := \{x \in G : (\forall g \in G)gx = xg\}.$$

Није тешко проверити да је $Z(G)$ једна подгрупа групе G. Наиме, како је $eg = ge$ за све $g \in G$, то $e \in Z(G)$. Ако $x, y \in Z(G)$, онда

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy),$$

па $xy \in Z(G)$. Осим тога, ако је $x \in Z(G)$, тј. за све $g \in G$ важи $xg = gx$, онда, множећи ову једнакост здесна и слева са x^{-1}, добијамо $gx^{-1} = x^{-1}g$. Закључујемо да и x^{-1} припада центру.

Веза између центра и конјугације дата је следећим ставом чији доказ следи непосредно из дефиниције центра.

Став 58 Центар групе G је унија свих једночланих класа конјугације.

Пример 59 Центар групе $\mathbb{D}_n$ је тривијалан уколико је n непаран број, а једнак је $\{\varepsilon, \rho^{n/2}\}$ уколико је n паран број.

Претпоставимо да је елемент $\sigma\rho^k$ у центру групе $\mathbb{D}_n$. То значи да је

$$(\sigma\rho^k)\rho = \rho(\sigma\rho^k),$$

тј.

$$\sigma\rho^{k+1} = \sigma\rho^{k-1}.$$

Одавде следи да је $\rho^2 = \varepsilon$, што није могуће. Дакле, можемо да закључимо да ниједан елемент облика $\sigma\rho^k$ не може бити у $Z(\mathbb{D}_n)$.

Посматрајмо елементе облика ρ^k за $1 \leq k < n$. Уколико је неки такав елемент у центру, мора бити

$$\rho^k(\sigma\rho) = (\sigma\rho)\rho^k,$$

па је

$$\sigma\rho^{-k}\rho = \sigma\rho^{k+1}.$$

Добијамо да мора бити $\rho^{2k} = \varepsilon$. Како је $n = \omega(\rho)$, добијамо да $n \mid 2k$. Уколико је n непаран, добили бисмо да $n \mid k$, што није могуће ($1 \leq k < n$). Дакле, центар групе $\mathbb{D}_n$ је тривијалан уколико је n непаран број. Уколико је пак n паран, онда $(n/2) \mid k$. Но, с обзиром да је $k < n$, закључујемо да мора бити $k = n/2$. Није тешко проверити (учините то!) да је у овом случају елемент $\rho^{n/2}$ заиста у центру. Дакле, за парне n је $Z(\mathbb{D}_n) = \{\varepsilon, \rho^{n/2}\}$. ♣

Напомена. Центар групе $\mathbb{D}_n$ могли смо да одредимо и из чињенице да знамо класе конјугације (центар је унија једночланих класа конјугације), али је добро то урадити и директно.

Дефиниција 60 Централизатор елемента $g \in G$, у ознаци, $Z(g)$ је скуп свих елемената групе G који комутирају са g:

$$Z(g) := \{x \in G : xg = gx\}.$$

Став 61 Важи следеће: а) $Z(g) \leq G$;

б) број елемената у класи конјугације елемента $g \in G$ једнак је индексу његовог централизатора.

Доказ. Провера чињенице да је $Z(g)$ подгрупа групе G изводи се на потпуно аналоган начин провери да је $Z(G)$ подгрупа.

Означимо са $C(g)$ класу конјугације елемента g. Другим речима,

$$C(g) = \{xgx^{-1} : x \in G\}.$$

Дефинишемо функцију $f : G/Z(g) \to C(g)$, са

$$f(xZ(g)) = xgx^{-1}.$$

Докажимо да је f добро дефинисана. Дакле, нека је $xZ(g) = yZ(g)$. Треба показати да је $xgx^{-1} = ygy^{-1}$. Но, како је $xZ(g) = yZ(g)$, то је $y^{-1}x \in Z(g)$, па је

$$(y^{-1}x)g = g(y^{-1}x).$$

Множењем ове једнакости слева са y, а здесна са x^{-1} и коришћењем асоцијативности множења добијамо тражени резултат (проверите!).

Јасно је да је f „на". Докажимо да је f „1–1". Нека је $f(xZ(g)) = f(yZ(g))$, тј. $xgx^{-1} = ygy^{-1}$. Одавде следи да је $(x^{-1}y)g = g(x^{-1}y)$, тј. $x^{-1}y \in Z(g)$, па је $xZ(g) = yZ(g)$. □

Последица 62 Свака коначна група реда p^n, где је p прост број, а $n \geq 2$, има нетривијалан центар.

Доказ. Као и у случају сваке релације еквиваленције, група G је дисјунктна унија различитих класа конјугације. Осим тога, центар групе G је унија свих једночланих класа конјугације. Добијамо да је

$$G = Z(G) \sqcup C_1 \sqcup \ldots \sqcup C_k, \tag{1}$$

при чему класе C_i нису једночлане. Другим речима,

$$|G| = |Z(G)| + |C_1| + \cdots + |C_k|,$$

при чему је $|C_i| > 1$. Како је $|C_i|$ једнако индексу централизатора (неког) елемента из C_i и како је $|C_i| \neq 1$, мора бити $p \mid |C_i|$. Из (**??**) следи да $p \mid |Z(G)|$, па центар заиста није тривијалан. □

Последица 63 Ако је p прост број, онда је свака група реда p^2 или циклична или изоморфна групи $\mathbb{Z}_p \times \mathbb{Z}_p$.

Доказ. Уколико у G постоји елемент реда p^2, група G је циклична. Претпоставимо да у G нема елемената реда p^2. Како према претходном $Z(G)$ није тривијална група, закључујемо да постоји $x \in Z(G) \setminus \{e\}$, који је нужно реда p. Нека је $H = \langle x \rangle$. Уколико је y ма који елемент из $G \setminus \langle x \rangle$, онда је y такође реда p и нека је $K = \langle y \rangle$. Како је $H \subseteq Z(G)$, сваки елемент из H комутира са сваким из K. Осим тога, ако је $H \cap K \neq \{e\}$, онда је $|H \cap K| = p$, па је $H = H \cap K = K$, што противречи претпоставци. Дакле, $H \cap K = \{e\}$. Уколико још докажемо да је $H \cdot K = G$, према ставу о разлагању на производ, добијамо да је $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Јасно је да је

$$H \cdot K = \{x^r y^s : 0 \leq r < p, 0 \leq s < p\}.$$

Показаћемо да међу овим елементима нема једнаких. Како их има $p^2 = |G|$, одатле добијамо да је $G = H \cdot K$. Претпоставимо да је

$$x^r y^s = x^t y^u$$

и да је, на пример, $r \geq t$. Добијамо:

$$x^{r-t} = y^{u-s}.$$

Тај елемент је и у H и у K. Како је пресек ових подгрупа тривијалан, закључујемо да је $x^{r-t} = e = y^{u-s}$. Но, како је $0 \leq r - t < p = \omega(x)$, закључујемо да је $r - t = 0$, тј. $r = t$. Следи да је и $s = u$, те међу наведеним елементима заиста нема једнаких. Дакле, $G = H \cdot K$, те је доказ завршен. □

Нормалне подгрупе и количничке групе

У случају да је $H \leq G$ разматрали смо скуп G/H, скуп свих левих косета подгрупе H у групи G. Испоставља се да се у неким случајевима на овом скупу може задати структура групе. Уведимо најпре следећу дефиницију.

Дефиниција 64 Подгрупа H групе G је нормална уколико је H унија неких класа конјугације. Ако је H нормална подгрупа од G онда пишемо:

$$H \triangleleft G.$$

Став 65 Нека је $H \leq G$. Следећи услови су еквивалентни:

1. $H \triangleleft G$;
2. за све $g \in G$: $gHg^{-1} \subseteq H$;
3. за све $g \in G$: $gH = Hg$.

Доказ.

$1 \implies 2$. Нека су $g \in G$ и $h \in H$ произвољни. Елемент ghg^{-1} је конјугат елемента $h \in H$. Како је H нормална подгрупа, она је унија класа конјугације, па самим тим мора да садржи целу класу конјугације елемента h. Стога је и $ghg^{-1} \in H$.

$2 \implies 3$. Нека је $g \in G$ произвољан елемент. Докажимо да је $gH \subseteq Hg$. Посматрајмо елемент $h \in H$. На основу 2, $ghg^{-1} \in H$, па је $ghg^{-1} = h'$ за неко $h' \in H$. Но, тада је и $gh = h'g \in Hg$, па закључујемо да је $gH \subseteq Hg$. Обратно, уочимо елемент $hg \in Hg$. Елемент $g^{-1}h(g^{-1})^{-1}$ на основу 2 припада H, па је $g^{-1}h(g^{-1})^{-1} = h_1$ за неко $h_1 \in H$. Стога је $hg = gh_1 \in gH$, те је $Hg \subseteq gH$.

$3 \implies 1$. Претпоставимо да је C нека класа конјугације за коју је $C \cap H \neq \emptyset$. Треба доказати да је $C \subseteq H$. Узмимо елемент $h \in C \cap H$. Тада је сваки елемент из C облика ghg^{-1} за неки $g \in G$. Но, како је по 3, $gH = Hg$, то је $gh = h'g$ за неко $h' \in H$, па је $ghg^{-1} = h'gg^{-1} = h'$. Закључујемо да $ghg^{-1} \in H$. Дакле, заиста је $C \subseteq H$. □

Приметимо да, у случају да је $H \triangleleft G$, важи једнакост $gHg^{-1} = H$.

Став 66 Свака подгрупа индекса 2 је нормална.

Доказ. Нека је $H \leq G$ и $[G : H] = 2$. То значи да је за сваки елемент $a \notin H$ из G испуњено:

$$G = H \sqcup aH.$$

Но, такође је и

$$G = H \sqcup Ha.$$

Како је $aH \cap H = \emptyset$, мора бити $aH \subseteq Ha$. Но, из истих разлога је $Ha \subseteq aH$. Закључујемо да је $aH = Ha$ за све $a \in G \setminus H$. Ако пак $a \in H$, онда је $aH = H$ (H је подгрупа, па је производ ма која два елемента из H у H; осим тога, ако је $h \in H$ произвољан елемент, онда је $h = a(a^{-1}h) \in aH$), а такође је и $Ha = H$. Дакле, и у овом случају важи једнакост $aH = Ha$, па је $H \triangleleft G$. □

Пример 67 Важи следеће:

1. за све $n \geq 2$: $\mathbb{A}_n \triangleleft \mathbb{S}_n$;
2. за сваку групу G: $\{e\} \triangleleft G$;
3. за сваку групу G: $G \triangleleft G$;
4. за сваку групу G: $Z(G) \triangleleft G$;
5. за све $n \geq 3$: $\langle \rho \rangle \triangleleft \mathbb{D}_n$.

У случају да су X и Y подскупови од G, дефинишемо $X \cdot Y$ са:

$$X \cdot Y := \{x \cdot y : x \in X, y \in Y\}.$$

Став 68 Скуп свих левих косета нормалне подгрупе H групе G чини једну групу у односу на управо дефинисано множење подскупова од G.

Доказ. Нека су aH и bH произвољни косети. Докажимо да је, при услову да је $H \triangleleft G$,

$$(aH) \cdot (bH) = (ab)H.$$

Ово није тешко доказати. Наиме, приметимо да је $HH = H$. Јасно је да је $HH \subseteq H$ (производ два елемента из H такође је у H пошто је H подгрупа од G). Осим тога, како $e \in H$, добијамо $H = eH \subseteq HH$. Добијамо:

$$(aH) \cdot (bH) = a(Hb)H = a(bH)H = (ab)(HH) = (ab)H.$$

Овде смо користили чињеницу да је $H \triangleleft G$ и асоцијативност множења.

Сада није тешко показати да је $(G/H, \cdot)$ група. Наиме,

$$((aH) \cdot (bH)) \cdot (cH) = ((ab)H) \cdot (cH) =$$

$$= ((ab)c)H = (a(bc))H = (aH) \cdot ((bc)H) = (aH) \cdot ((bH) \cdot (cH)).$$

Јасно је да је $H = eH$ неутрал:

$$(aH) \cdot H = (aH) \cdot (eH) = (ae)H = aH,$$

као и

$$H \cdot (aH) = (eH) \cdot (aH) = (ea)H = aH.$$

Инверз елемента aH је $a^{-1}H$:

$$(aH)\cdot(a^{-1}H) = (aa^{-1})H = eH = H;$$

$$(a^{-1}H)\cdot(aH) = (a^{-1}a)H = eH = H.$$

□

Овако добијена група зове се количничка група групе G по нормалној подгрупи H. Убудуће, када говоримо о групи G/H подразумевамо да је H нормална подгрупа од G и да је множење косета дефинисано на наведени начин. Наравно, често нећемо писати неке непотребне заграде и знак множења.

Дефиниција 69 Група G је проста уколико су њене једине нормалне подгрупе G и $\{e\}$.

Уколико група G није комутативна, то не мора бити ни њена количничка група. Ипак има случајева у којима количничка група јесте комутативна, а сама група то није.

Дефиниција 70 Ако су $x, y \in G$, дефинишемо комутатор елемената x и y, у ознаци $[x, y]$ са:

$$[x, y] := x^{-1}y^{-1}xy.$$

Приметимо да је $xy = yx$ акко $[x, y] = e$. Подгрупу групе G генерисану комутаторима означавамо са $[G, G]$ и зовемо комутаторска подгрупа од G. Осим ове ознаке, појављује се и ознака G' (те се за ту подгрупу каже и да је извод групе G).

Став 71 а) Комутаторска подгрупа је нормална подгрупа.

б) Ако је $H \triangleleft G$, онда је G/H комутативна ако и само ако је $[G, G] \subseteq H$.

Доказ. а) Производ два комутатора не мора бити комутатор, али инверз ма ког комутатора јесте комутатор:

$$[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}(y^{-1})^{-1}(x^{-1})^{-1} = y^{-1}x^{-1}yx = [y, x].$$

У сваком случају, ми посматрамо подгрупу генерисану комутаторима и треба да покажемо да је она нормална. Сваки елемент подгрупе генерисане неким скупом X је скуп свих могућих производа елемената из X и њихових инверза. Како је инверз комутатора и сам комутатор, то је сваки елемент из комутаторске групе производ комутатора. Стога, нека су $g, x_1, y_1, \ldots, x_n, y_n$ произвољни елементи групе G. Тада је

$$g[x_1, y_1][x_2, y_2]\cdots[x_n, y_n]g^{-1} = (g[x_1, y_1]g^{-1})(g[x_2, y_2]g^{-1})\cdots(g[x_n, y_n]g^{-1})$$

Но,

$$g[x, y]g^{-1} = gx^{-1}y^{-1}xyg^{-1} = (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) =$$

$$= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) = [gxg^{-1}, gyg^{-1}],$$

те добијамо

$$g[x_1, y_1]\cdots[x_n, y_n]g^{-1} = [gx_1g^{-1}, gy_1g^{-1}]\cdots[gx_ng^{-1}, gy_ng^{-1}] \in [G, G].$$

б) $\Rightarrow$: Претпоставимо да је група G/H комутативна. То значи да је за све $x, y \in G$ испуњено:

$$xH \cdot yH = yH \cdot xH.$$

Другим речима,

$$xyH = yxH,$$

па мора бити

$$(yx)^{-1}(yx) \in H,$$

те

$$[x, y] = x^{-1}y^{-1}xy \in H.$$

Дакле, комутатор ма која два елемента је у H, па закључујемо да је $[G, G] \subseteq H$.

$\Leftarrow$: Претпоставимо да је $[G, G] \subseteq H$. Треба показати да је група G/H комутативна. Нека су $x, y \in G$ произвољни елементи. По претпоставци $[x, y] \in H$, тј. $x^{-1}y^{-1}xy \in H$. То значи да је $(yx)^{-1}(xy) \in H$, па мора бити $(yx)H = (xy)H$, тј. $(yH) \cdot (xH) = (xH) \cdot (yH)$. Закључујемо да је G/H комутативна група. □

Група $G/[G, G]$ назива се Абелизација групе G и означава са G^{Ab} (комутативне групе називају се и Абелове групе). Понеки пут је погодно за испитивање да ли су две групе изоморфне прећи на њихове Абелизације, зато што важи следећи став.

Став 72 Ако је $G \cong H$ онда је и $G^{\mathrm{Ab}} \cong H^{\mathrm{Ab}}$.

Нека је $f\colon G \to H$ изоморфизам. Тада је $f([x, y]) = [f(x), f(y)]$, што се лако може установити. Одавде следи да

$$f\,[[G, G]] \subseteq [H, H]. \tag{2}$$

Дефинишимо функцију

$$\tilde{f}\colon G^{\mathrm{Ab}} \to H^{\mathrm{Ab}},$$

са:

$$\tilde{f}(x[G, G]) := f(x)[H, H].$$

Показаћемо даје $\tilde{f}$ добро дефинисана функција, која остварује изоморфизам између $G/[G, G]$ и $H/[H, H]$.

Добра дефинисаност: Нека је

$$x[G, G] = y[G, G].$$

Треба показати да је

$$f(x)[H,H] = f(y)[H,H].$$

Но, како је $x[G,G] = y[G,G]$, мора бити $x^{-1}y \in [G,G]$, па на основу (**??**) следи да $f(x)^{-1}f(y) = f(x^{-1}y) \in [H,H]$. Дакле, заиста је

$$f(x)[H,H] = f(y)[H,H].$$

$\tilde{f}$ је „на": Нека је $z[H,H]$ произвољан елемент из H^{Ab}. Како је f „на", то постоји $x \in G$ за који је $f(x) = z$. Но, тада је $\tilde{f}(x[G,G]) = f(x)[H,H] = z[H,H]$, па је $\tilde{f}$ заиста „на".

$\tilde{f}$ је „1–1": Ако је

$$\tilde{f}(x[G,G]) = \tilde{f}(y[G,G]),$$

то значи да је

$$f(x)[H,H] = f(y)[H,H],$$

па је

$$f(x^{-1}y) \in [H,H].$$

Другим речима, за неке $z_1, u_1, \ldots, z_n, u_n \in H$ је

$$f(x^{-1}y) = [z_1,u_1]\cdots[z_n,u_n].$$

Како је f „на", то постоје $x_1, y_1, \ldots, x_n, y_n \in G$ такви да је

$$f(x_1) = z_1, \ldots, f(x_n) = z_n, \quad f(y_1) = u_1, \ldots, f(y_n) = u_n.$$

То значи да је

$$f(x^{-1}y) = [f(x_1),f(y_1)]\cdots[f(x_n),f(y_n)] = f([x_1,y_1]\cdots[x_n,y_n]).$$

Како је f „1–1", мора бити

$$x^{-1}y = [x_1,y_1]\cdots[x_n,y_n].$$

Следи да $x^{-1}y \in [G,G]$, па је $x[G,G] = y[G,G]$ и закључујемо да је и функција $\tilde{f}$ „1–1".

$\tilde{f}$ се слаже са операцијама:

$$\tilde{f}((x[G,G])\cdot(y[G,G])) = \tilde{f}((xy)[G,G]) = f(xy)[H,H] = (f(x)f(y))[H,H] =$$

$$= (f(x)[H,H])(f(y)[H,H]) = \tilde{f}(x[G,G])\tilde{f}(x[G,G]).$$

Закључујемо да је $\tilde{f}$ заиста изоморфизам. □

Пример 73 За све $n \geq 2$: $\mathbb{S}_n^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

Показаћемо да је $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$ за све $n \geq 2$. Јасно је да је $\pi^{-1}\sigma^{-1}\pi\sigma$ парна пермутација за сваке две пермутације π и σ (зашто?). Према томе, $[\mathbb{S}_n, \mathbb{S}_n] \subseteq \mathbb{A}_n$.

Случај $n = 2$ је тривијалан. Претпоставимо стога да је $n \geq 3$. Докажимо да сваки цикл дужине 3 припада $[\mathbb{S}_n, \mathbb{S}_n]$. Како ти цикли генеришу $\mathbb{A}_n$, добићемо да је $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$. Но,

$$(abc) = (ab)(bc) = (ab)(ac)(ab)(ac) = (ab)^{-1}(ac)^{-1}(ab)(ac) = [(ab), (ac)].$$

Како је $[\mathbb{S}_n : \mathbb{A}_n] = 2$, то је група $\mathbb{S}_n/\mathbb{A}_n$ реда 2 и као таква је изоморфна групи $\mathbb{Z}_2$. ♣

Пример 74 За све $s \geq 2$:

1. $(\mathbb{D}_{2s})^{\mathrm{Ab}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$;
2. $(\mathbb{D}_{2s-1})^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

Показаћемо најпре да је $[\mathbb{D}_n, \mathbb{D}_n] = \langle \rho^2 \rangle$. Проверимо све случајеве:

1. $[\rho^k, \rho^l] = \varepsilon$;
2. $[\sigma\rho^k, \rho^l] = (\sigma\rho^k)^{-1}(\rho^l)^{-1}(\sigma\rho^k)\rho^l = \sigma\rho^k\rho^{-l}\sigma\rho^k\rho^l = \rho^{-k}\rho^l\rho^{k+l} = \rho^{2l}$;
3. $[\rho^k, \sigma\rho^l] = (\rho^k)^{-1}(\sigma\rho^l)^{-1}\rho^k(\sigma\rho^l) = \rho^{-k}\sigma\rho^l\rho^k\sigma\rho^l = \rho^{-k}\rho^{-l}\rho^{-k}\rho^l = \rho^{-2k}$;
4. $[\sigma\rho^k, \sigma\rho^l] = (\sigma\rho^k)^{-1}(\sigma\rho^l)^{-1}\sigma\rho^k\sigma\rho^l = \sigma\rho^k\sigma\rho^l\sigma\rho^k\sigma\rho^l = \rho^{-k}\rho^l\rho^{-k}\rho^l = \rho^{2l-2k}$.

Видимо да је заиста $[\mathbb{D}_n, \mathbb{D}_n] = \langle \rho^2 \rangle$. Сада се разликују случајеви када је n парно, односно непарно. Наиме, ако је $n = 2s - 1$, ред елемента ρ^2 је n (зашто?), па је $\langle \rho^2 \rangle = \langle \rho \rangle$. Стога је $[\mathbb{D}_{2s-1}, \mathbb{D}_{2s-1}] = \langle \rho \rangle$ и заиста је $(\mathbb{D}_{2s-1})^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

У случају $n = 2s$, ред елемента ρ^2 је s и

$$(\mathbb{D}_{2s})^{\mathrm{Ab}} = \{\langle \rho^2 \rangle, \sigma\langle \rho^2 \rangle, \rho\langle \rho^2 \rangle, \sigma\rho\langle \rho^2 \rangle\}.$$

Ово је група са 4 елемента у којој је сваки елемент реда 2 (проверити ово!), па на основу ранијих резултата (а може и директно), добијамо да је $(\mathbb{D}_{2s})^{\mathrm{Ab}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. ♣

Докажимо на крају још један став, који нам даје карактеризацију група одређеног реда.

Став 75 Ако је p непаран прост број, онда је свака група реда $2p$ или циклична или је изоморфна групи $\mathbb{D}_p$.

Доказ. Нека је G група реда $2p$. На основу Кошијеве теореме, у групи G постоји елемент x реда p и елемент y реда 2. Како ред елемента дели ред групе, то $y \notin \langle x \rangle$. Стога је

$$G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, \ldots, x^{p-1}, y, yx, \ldots, yx^{p-1}\}.$$

Ред елемента yx може бити 2, p или $2p$ ($yx \neq e$). Уколико је $\omega(yx) = 2p$, група G је циклична.

Покажимо да $\omega(yx) \neq p$. Претпоставимо да је $\omega(yx) = p$. Тада добијамо (рачунамо у групи $G/\langle x\rangle$ — подгрупа $\langle x\rangle$ је нормална пошто је индекса 2):

$$\langle x\rangle = e\langle x\rangle = (yx)^p\langle x\rangle = (yx\langle x\rangle)^p = (y\langle x\rangle)^p = y^p\langle x\rangle.$$

Дакле, $y^p \in \langle x\rangle$. Како је p непаран број, а $\omega(y) = 2$, мора бити $y \in \langle x\rangle$, што није тачно. Добили смо контрадикцију, те можемо закључити да $\omega(yx) \neq p$. Остаје случај $\omega(yx) = 2$. Тада добијамо да је $(yx)^2 = e$, па је $yxyx = e$ из чега следи да је $yx = x^{-1}y$. С обзиром да је $x^p = e$ и $y^2 = e$, видимо да се изоморфизам између G и $\mathbb{D}_p$ може остварити придруживањем $y \mapsto \sigma$, $x \mapsto \rho$. □

Аутоморфизми група

Нека је G група. Са $\mathrm{Aut}(G)$ означавамо скуп свих аутоморфизама групе G:

$$\mathrm{Aut}(G) := \{f : G \to G \mid f \text{ је аутоморфизам}\}.$$

Како је композиција два аутоморфизма аутоморфизам, а и инверз аутоморфизма је аутоморфизам то је $(\mathrm{Aut}(G), \circ)$ једна група (идентично пресликавање је наравно аутоморфизам), коју зовемо *група аутоморфизама групе* G.

Нека $g \in G$. Дефинишимо $u_g : G \to G$ са:

$$u_g(x) = gxg^{-1}.$$

Није тешко уверити се да је u_g аутоморфизам групе G. Наиме,

$$u_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = u_g(x)u_g(y).$$

Осим тога,

$$(u_g \circ u_h)(x) = u_g(u_h(x)) = u_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = u_{gh}(x).$$

Дакле, $u_g \circ u_h = u_{gh}$. Како је, очигледно, $u_e = \mathrm{id}_G$, то добијамо да је, за свако $g \in G$: $u_g \circ u_{g^{-1}} = u_e = \mathrm{id}_G$. Закључујемо да је u_g бијекција и да је, заправо, $u_g^{-1} = u_{g^{-1}}$. На овај начин смо показали не само да је сваки u_g један аутоморфизам, него и да скуп свих аутоморфизама тог облика, чини једну подгрупу групе свих аутоморфизама. Аутоморфизме овог облика зваћемо *унутрашњи аутоморфизми* и користићемо ознаку

$$\mathrm{Inn}(G) := \{u_g \mid g \in G\},$$

за подгрупу свих унутрашњих аутоморфизама групе G.

Знамо да је $(\mathrm{Inn}(G), \circ) \leq (\mathrm{Aut}(G), \circ)$, но поставља се питање да ли је то и нормална подгрупа. Проверимо то. Нека је $\phi \in \mathrm{Aut}(G)$. Треба показати да је

$$\phi \circ \mathrm{Inn}(G) \circ \phi^{-1} \subseteq \mathrm{Inn}(G).$$

Нека $g \in G$. Тада за сваки $x \in G$:

$$\begin{aligned}(\phi \circ u_g \circ \phi^{-1})(x) &= \phi(u_g(\phi^{-1}(x))) \\ &= \phi(g\phi^{-1}(x)g^{-1}) \\ &= \phi(g)\phi(\phi^{-1}(x)\phi(g^{-1}) \\ &= \phi(g)x\phi(g)^{-1} \\ &= u_{\phi(g)}(x).\end{aligned}$$

Дакле, $\phi \circ u_g \circ \phi^{-1} = u_{\phi(g)} \in \mathrm{Inn}(G)$. Закључујемо да је $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

Количничку групу $\mathrm{Aut}(G)/\mathrm{Inn}(G)$, означавамо са $\mathrm{Out}(G)$ и зовемо *група спољашњих аутоморфизама групе* G (сваки косет у овој групи, различит од $\mathrm{Inn}(G)$, задат је неким аутоморфизмом који није унутрашњи, тј. који није задат неким конкретним елементом групе G као што је задат унутрашњи аутоморфизам).

Став 76 Придруживање

$$gZ(G) \mapsto u_g$$

представља изоморфизам група $G/Z(G)$ и $\mathrm{Inn}(G)$.

Доказ. Посматрамо функцију $\phi : G/Z(G) \to \mathrm{Inn}(G)$ задату са:

$$\psi(gZ(G)) = u_g.$$

Треба доказати да је ψ изоморфизам (како је $Z(G)$ нормална подгрупа од G, то заиста имамо количничку групу $G/Z(G)$).

Докажимо најпре да је ψ добро дефинисана. У ту сврху, нека је $gZ(G) = hZ(G)$. Треба показати да је $u_g = u_h$. Из $gZ(G) = hZ(G)$ следи да је $g^{-1}h \in Z(G)$, тј. да за сваки $x \in G$ важи

$$g^{-1}hx = xg^{-1}h.$$

Множењем ове једнакости слева са g, а здесна са h^{-1} добијамо да за сваки $x \in G$:

$$hxh^{-1} = gxg^{-1},$$

тј. да је за свако $x \in G$: $u_h(x) = u_g(x)$. Закључујемо да је заиста $u_g = u_h$.

На сличан начин се проверава да је ψ „1–1". Нека је $\psi(gZ(G)) = \psi(hZ(G))$. То значи да је $u_g = u_h$, те је за све $x \in G$: $u_g(x) = u_h(x)$. Дакле, за све $x \in G$ важи:

$$gxg^{-1} = hxh^{-1}.$$

Множењем ове једнакости слева са g^{-1}, а здесна са h добијамо да за свако $x \in G$ важи:

$$g^{-1}hx = xg^{-1}h,$$

што заправо значи да $g^{-1}h \in Z(G)$, те закључујемо да је $gZ(G) = hZ(G)$. Тако смо добили да је ψ „1–1".

Функција ψ је очигледно „на" (зашто?), те нам само преостаје да покажемо да се слаже са операцијама, тј. да је за све $g, h \in G$

$$\psi((gZ(G))(hZ(G))) = \psi(gZ(G)) \circ \psi(hZ(G)).$$

(Присетимо се да је операција у $\mathrm{Inn}(G)$ заправо композиција функција.) Но,

$$\begin{aligned} \psi((gZ(G))(hZ(G))) &= \psi((gh)Z(G)) \\ &= u_{gh} \\ &= u_g \circ u_h \\ &= \psi(gZ(G)) \circ \psi(hZ(G)). \end{aligned}$$

□

Поставља се питање да ли група унутрашњих аутоморфизама може бити циклична. Наравно, уколико је група G комутативна, сваки унутрашњи аутоморфизам је идентитет (зашто?), те је тада $\mathrm{Inn}(G) = \{\mathrm{id}_G\}$, но то је тривијална група. Следећи став нам даје одговор на то питање.

Став 77 Група $\mathrm{Inn}(G)$ никада није (нетривијална) циклична група.

Доказ. Претпоставимо да је $\mathrm{Inn}(G)$ циклична група. На основу претходног става добијамо да је и $G/Z(G)$ циклична, тј. да постоји $x \in G$ за који је $G/Z(G) = \langle xZ(G) \rangle$. Показаћемо да одатле следи да је G комутативна група. У ту сврху, нека су y, z произвољни елементи из G. Како ј $xZ(G)$ генератор групе $G/Z(G)$, то постоје $m, n \in \mathbb{Z}$ за које је

$$yZ(G) = (xZ(G))^m \quad \text{и} \quad zZ(G) = (xZ(G))^n.$$

Но, то заправо значи да постоје $c, d \in Z(G)$ такви да је

$$y = x^m c \quad \text{и} \quad z = x^n d.$$

(Зашто?) Но, тада добијамо да је

$$\begin{aligned} yz &= x^m c x^n d \\ &= x^m x^n c d \quad (c \in Z(G)) \\ &= x^n x^m c d \\ &= x^n d x^m c \quad (d \in Z(G)) \\ &= zy. \end{aligned}$$

Дакле, G је комутативна група, па је $G = Z(G)$, те је $G/Z(G)$ тривијална група, те је тривијална и група $\mathrm{Inn}(G)$. □

Одређивање групе аутоморфизама произвољне групе није лак задатак, стога ћемо се ми овде ограничити само на неке једноставније случајеве и примере.

Позабавимо се најпре питањем одређивања групе аутоморфизама цикличне групе.

Свака бесконачна циклична група изоморфна је групи $\mathbb{Z}$. Није тешко уверити се да су једини аутоморфизми ове групе идентитет и $x \mapsto -x$ (проверите ово). Стога је $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

Нека је $n \geq 2$ и $f \in \mathrm{Aut}(\mathbb{Z}_n)$ (како је јасно да из $G \cong H$ следи да је $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$ (уверите се у то!), као и да је свака нетривијална коначна циклична група изоморфна тачно једној групи $\mathbb{Z}_n$, за $n \geq 2$, ми разматрамо тај случај). Елемент 1 је генератор групе $\mathbb{Z}_n$ и аутоморфизам f је потпуно одређен сликом елемента 1. Наиме, нека је $f(1) = r$. Уколико је $x \in \mathbb{Z}_n$, то је

$$x = \underbrace{1 +_n \cdots +_n 1}_{x},$$

те добијамо

$$f(x) = f(\underbrace{1 +_n \cdots +_n 1}_{x}) = \underbrace{f(1) +_n \cdots +_n f(1)}_{x} = \underbrace{r +_n \cdots +_n r}_{x}.$$

Но,

$$\underbrace{r +_n \cdots +_n r}_{x} = r \cdot_n x.$$

Наиме, и лева и десна страна ове једнакости су заправо остатак при дељењу rx са n. Према томе, добијамо да је за свако $x \in \mathbb{Z}_n$:

$$f(x) = r \cdot_n x.$$

Дакле, из чињенице да се f слаже са операцијама видели смо каквог је облика f. Поставља се питање: какво мора бити $r \in \mathbb{Z}_n$ да са $x \mapsto r \cdot_n x$ буде задат аутоморфизам групе $\mathbb{Z}_n$? Пре свега, с обзиром на својства операција $+_n$ и $\cdot_n$, овакво придруживање увек се слаже са операцијом. Како је група $\mathbb{Z}_n$ коначна, то је довољно проверити за које r је овакво придруживање „на" (зашто?). Но, то није тешко. Довољно је испитати када је 1 слика неког елемента (пошто је 1 генератор групе $\mathbb{Z}_n$). То значи да треба установити за које $r \in \mathbb{Z}_n$ постоји $s \in \mathbb{Z}_n$ тако да је $r \cdot_n s = 1$. Но, добро нам је познато да то важи ако и само ако је r узајамно просто са n. Подсетимо се да смо са $\Phi(n)$ означили све елементе из скупа $\{1, \ldots, n-1\}$ који су узајамно прости са n. Дакле, придруживање $x \mapsto r \cdot_n x$ задаје аутоморфизам групе $\mathbb{Z}_n$ ако и само ако $r \in \Phi(n)$. Но, $(\Phi(n), \cdot_n)$ је група и на основу претходног разматрања, може се очекивати да постоји веза ове групе и групе $\mathrm{Aut}(\mathbb{Z}_n)$. Заправо важи следећи став.

Став 78 Функција $\Psi\colon \mathrm{Aut}(\mathbb{Z}_n) \to \Phi(n)$, задата са:

$$\Psi(f) = f(1)$$

је изоморфизам група $(\mathrm{Aut}(G), \circ)$ и $(\Phi(n), \cdot_n)$.

Доказ. На основу претходног разматрања, Ψ је бијекција (зашто?). Потребно је само проверити слагање са операцијама. Но, то није тешко:

$$\begin{aligned}\Psi(f \circ g) &= (f \circ g)(1)\\ &= f(g(1))\\ &= f(1) \cdot_n g(1).\end{aligned}$$

(користили смо доказани резултат по коме је $f(x) = f(1) \cdot_n x$ за аутоморфизам f и елемент x). Овим је доказ завршен. □

Погледајмо сада неке примере.

Пример 79 Показати да је $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathbb{S}_3$.

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$. Сви елементи ове групе (сем неутрала) су реда 2. Означимо са X скуп свих елемената реда 2 у овој групи. Посматрајмо функцију

$$\Psi\colon \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \to \mathbb{S}_X,$$

дефинисану са:

$$\Psi(\phi) := \phi|_X.$$

Јасно је да је ово добро дефинисана функција пошто аутоморфизам не мења ред елемента, па је заиста $\phi[X] = X$ за сваки аутоморфизам ϕ (пажљив читалац ће приметити да ово није баш права рестрикција, пошто при рестрикцији „смањујемо" само домен, а не и кодомен, али јасно је шта желимо да урадимо). Сваки аутоморфизам је потпуно одређен вредностима у елементима реда 2, пошто се неутрал обавезно слика у неутрал. Стога је Ψ „1–1". Но, Ψ је и „на" пошто свака пермутација скупа X задаје један аутоморфизам (производ свака два различита елемента из X једнак је трећем елементу). Стога је Ψ и „на". С обзиром да је у обе групе операција $\circ$, то се Ψ слаже и са операцијом, те је заиста један изоморфизам. Како је X скуп од три елемента, то је тврђење доказано. ♣

Пример 80 Одредити групу $\mathrm{Aut}(\mathbb{S}_3)$.

$\mathbb{S}_3 = \{(1),(12),(13),(23),(123),(132)\}$. Нека је $X = \{(12),(13),(23)\}$. Као и у претходном примеру, пошто су у X сви елементи реда 2 у групи $\mathbb{S}_3$, то за сваки $\phi \in \mathrm{Aut}(\mathbb{S}_3)$ важи: $\phi[X] = X$. Осим тога, вредности

које аутоморфизам „узима" на елементима скупа X јединствено одређују тај аутоморфизам (елементи из X генеришу $\mathbb{S}_3$). И не само то – вредности на скупу X могу се узети произвољно и тако добити један аутоморфизам (размислите и проверите на примеру!). Дакле, као и у претходном примеру, „рестрикција" задаје изоморфизам група $\mathrm{Aut}(\mathbb{S}_3)$ и S_X, па је $\mathrm{Aut}(\mathbb{S}_3) \cong \mathbb{S}_3$. ♣

Напомена. Приметимо да групе $\mathbb{Z}_2 \times \mathbb{Z}_2$ и $\mathbb{S}_3$ нису изоморфне, али њихове групе аутоморфизама то јесу.

Нека су G и H произвољне групе. Ако је $\phi \in \mathrm{Aut}(G)$ и $\psi \in \mathrm{Aut}(H)$, онда је лако проверити да је функција $\phi \times \psi$, дефинисана са:

$$(\phi \times \psi)(g, h) = (\phi(g), \psi(h)),$$

за $g \in G$ и $h \in H$ аутоморфизам групе $G \times H$. Јасно је да у општем случају не мора сваки аутоморфизам групе $G \times H$ да буде тог облика (једини аутоморфизам групе $\mathbb{Z}_2$ је идентитет, а видели смо да је $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathbb{S}_3$). Следећи став нам даје довољне услове да сваки аутоморфизам буде овог облика.

Став 81 Нека је $|G| = m$, $|H| = n$ и нека су m и n узајамно прости. Тада је $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

Доказ. Главни део доказа састоји се у томе да се покаже да је при датим условима сваки аутоморфизам $\Theta \in \mathrm{Aut}(G \times H)$ облика $\phi \times \psi$, за неки ϕ из $\mathrm{Aut}(G)$ и неки ψ из $\mathrm{Aut}(H)$. Нека је e неутрал у G и ε неутрал у H. Тврдимо да важи следеће:

$$\Theta(g, \varepsilon) = (\phi(g), \varepsilon),$$

где је ϕ неки аутоморфизам групе G. Претпоставимо да је за неко $g \in G$ испуњено: $\Theta(g, \varepsilon) = (\phi(g), h_0)$, где је h_0 елемент из H различит од неутрала (јасно је да је прва компонента задата *неком* функцијом од g – касније ћемо показати да је задата аутоморфизмом). Како је $m = |G|$, то је $g^m = e$ и добијамо да је $(g, \varepsilon)^m = (e, \varepsilon)$. Стога је

$$(\phi(g), h_0)^m = \Theta(g, \varepsilon)^m = \Theta((g, \varepsilon)^m) = \Theta(e, \varepsilon) = (e, \varepsilon).$$

Дакле, $h_0^m = e$. Стога $\omega(h_0) \mid m$. Како $h_0 \in H$, а $|H| = n$, то важи и $\omega(h_0) \mid n$. По претпоставци је $h_0 \neq \varepsilon$, те је $\omega(h_0) \neq 1$. Добијамо да m и n имају заједнички делилац већи од 1, што противречи претпоставци да су узајамно прости. То показује да је заиста

$$\Theta(g, \varepsilon) = (\phi(g), \varepsilon)$$

за све $g \in G$. Приметимо да ϕ мора бити „1–1", јер је Θ „1–1". Како је G коначна група, следи да је ϕ и „на". Но, ϕ се слаже и са операцијама:

$$(\phi(g_1 g_2), \varepsilon) = \Theta(g_1 g_2, \varepsilon\varepsilon) = \Theta(g_1, \varepsilon)\Theta(g_2, \varepsilon) = (\phi(g_1), \varepsilon)(\phi(g_2), \varepsilon) = (\phi(g_1)\phi(g_2), \varepsilon),$$

па је заиста $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$.

На потпуно исти начин се показује да је

$$\Theta(e, h) = (e, \psi(h)),$$

за неки $\psi \in \mathrm{Aut}(H)$. Коначно добијамо:

$$\Theta(g, h) = \Theta((g, \varepsilon)(e, h)) = \Theta(g, \varepsilon)\Theta(e, h) = (\phi(g), \varepsilon)(e, \psi(h)) = (\phi(g), \psi(h)).$$

Сада је лако проверити да је један изоморфизам

$$F\colon \mathrm{Aut}(G \times H) \to \mathrm{Aut}(G) \times \mathrm{Aut}(H)$$

задат са $F(\phi, \psi) = \phi \times \psi$. Остављамо читаоцима да ово провере. □

Овај резултат, уз раније резултате о аутоморфизмима цикличних група има једну, помало неочекивану последицу.

Последица 82 Нека су m и n узајамно прости природни бројеви. Тада је $\varphi(mn) = \varphi(m)\varphi(n)$.

Доказ. Присетимо се да је $\varphi(n) = |\Phi(n)|$, где је $\Phi(n) = \{k : 1 \leq k < n,\ \mathrm{NZD}(k, n) = 1\}$. Како су m и n узајамно прости, имамо изоморфизам $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Стога је

$$\Phi(mn) \cong \mathrm{Aut}(\mathbb{Z}_{mn}) \cong \mathrm{Aut}(\mathbb{Z}_m \times \mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_m) \times \mathrm{Aut}(\mathbb{Z}_n) \cong \Phi(m) \times \Phi(n).$$

Добијамо $\varphi(mn) = |\Phi(mn)| = |\Phi(m) \times \Phi(n)| = |\Phi(m)||\Phi(n)| = \varphi(m)\varphi(n)$. □

Наравно, овде смо у доказу користили једноставну чињеницу да из $G \cong G_1$ и $H \cong H_1$ следи $G \times H \cong G_1 \times H_1$. Докажите је за вежбу.

Хомоморфизми и теореме о изоморфизмима

Већ смо упознати са појмом изоморфизма група. Општији појам је појам хомоморфизма.

Дефиниција 83 Нека су $(G, \cdot)$ и $(H, *)$ групе. Функција $f\colon G \to H$ је хомоморфизам уколико за све $x, y \in G$ важи:

$$f(x \cdot y) = f(x) * f(y).$$

Дакле, изоморфизам је онај хомоморфизам који је и бијекција. Приметимо да се лако показује, на исти начин као и у случају изоморфизма, да се при сваком хомоморфизму неутрал групе G слика у неутрал групе H, а инверз елемента из групе G у инверз његове слике у групи H (подсетите се тог доказа). Како хомоморфизам не мора бити бијекција, природно је испитати у којој мери дати хомоморфизам „одступа" од изоморфизма. Важан појам у вези са тим је и појам *језгра* хомоморфизма.

Дефиниција 84 Нека је $f: G \to H$ хомоморфизам група. Језгро хомоморфизма f, у ознаци $\mathrm{Ker}(f)$ дефинише се са:

$$\mathrm{Ker}(f) := \{g \in G : f(g) = e_H\},$$

где је са e_H означен неутрал у H.

Став 85 Језгро сваког хоморфизма $f: G \to H$ је нормална подгрупа групе G.

Доказ. Како је $f(e_G) = e_H$, то $e_G \in \mathrm{Ker}(f)$, па $\mathrm{Ker}(f) \neq \emptyset$. Претпоставимо да $x, y \in \mathrm{Ker}(f)$. Треба показати да $x^{-1}y \in \mathrm{Ker}(f)$. Но,

$$f(x^{-1}y) = f(x)^{-1} * f(y) = e_H^{-1} * e_H = e_H,$$

те заиста $x^{-1}y \in \mathrm{Ker}(f)$. Дакле, доказали смо да је $\mathrm{Ker}(f) \leq G$.

Да бисмо показали да је језгро нормална подгрупа, посматрајмо произвољне елементе $x \in \mathrm{Ker}(f)$ и $g \in G$. Тада је

$$f(gxg^{-1}) = f(g) * f(x) * f(g)^{-1} = f(g) * e_H * f(g)^{-1} = e_H,$$

те закључујемо да је $g\mathrm{Ker}(f)g^{-1} \subseteq \mathrm{Ker}(f)$, за све $g \in G$, те је заиста $\mathrm{Ker}(f) \triangleleft G$. □

Став 86 Хомоморфизам група $f: G \to H$ је „1–1" ако и само ако је

$$\mathrm{Ker}(f) = \{e_G\}.$$

Доказ.
$\Longrightarrow$: Претпоставимо да је f „1–1" и нека $x \in \mathrm{Ker}(f)$. То значи да је

$$f(x) = e_H = f(e_G).$$

Како је f „1–1", мора бити $x = e_G$. Закључујемо да је $\mathrm{Ker}(f) = \{e_G\}$.

$\Longleftarrow$: Нека је $\mathrm{Ker}(f) = \{e_G\}$. Претпоставимо да је $f(x) = f(y)$. То значи да је

$$f(x^{-1}y) = f(x^{-1}) * f(y) = f(x)^{-1} * f(y) = e_H^{-1} * e_H = e_H,$$

па је $x^{-1}y \in \mathrm{Ker}(f) = \{e_G\}$. Добијамо да је $x = y$, те закључујемо да је f „1–1". □

Уколико је $\mathrm{Ker}(f) = \{e_G\}$, кажемо и да је језгро тривијално. Ако је f „1–1" хомоморфизам, кажемо и да је f *мономорфизам*.

Дефиниција 87 Слика хомоморфизма $f: G \to H$, у ознаци $\mathrm{Im}(f)$, дефинише се са:

$$\mathrm{Im}(f) := \{y \in H : (\exists x \in G) y = f(x)\}.$$

Дакле, слика хоморфизма је заправо обична слика функције f.

Став 88 Ако је $f\colon G \to H$ хомоморфизам, онда је $\mathrm{Im}(f) \leq H$.

Доказ. Како је $e_H = f(e_G)$, то $\mathrm{Im}(f) \neq \emptyset$. Претпоставимо да $y_1, y_2 \in \mathrm{Im}(f)$. То значи да постоје x_1, x_2 такви да је $f(x_1) = y_1$ и $f(x_2) = y_2$. Но, тада је

$$y_1^{-1} * y_2 = f(x_1)^{-1} * f(x_2) = f(x_1^{-1}x_2) \in \mathrm{Im}(f).$$

□

Приметимо да слика хомоморфизма не мора бити нормална подгрупа од H. Наиме, ако је $H \leq G$ онда је слика од H при инклузији (која је хомоморфизам) сама подгрупа H и ако она није нормална, то нам даје тражени пример.

Хомоморфизам, који је уједно и „на", зовемо *епиморфизам*. Основни пример епиморфизма је следећи. Нека је G група и H ма која њена нормална подгрупа. Тада је са $p(a) = aH$ задат један *епиморфизам* $p\colon G \to G/H$. Наравно, јасно је да је p „на". Осим тога

$$p(ab) = (ab)H = (aH)(bH) = p(a)p(b),$$

те је p и хомоморфизам.

Наведимо сада прву теорему о изоморфизмима група.

Теорема 89 (Прва теорема о изоморфизмима група) Нека је $f\colon G \to H$ хомоморфизам група. Тада f индукује изоморфизам $\tilde{f}\colon G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ дефинисан са: $\tilde{f}(x\,\mathrm{Ker}(f)) := f(x)$.

Доказ. Покажимо најпре да је $\tilde{f}$ добро дефинисана функција. Наиме, нека је $x\,\mathrm{Ker}(f) = y\,\mathrm{Ker}(f)$. То значи да $x^{-1}y \in \mathrm{Ker}(f)$. Дакле, $f(x^{-1}y) = e_H$, па је $f(x) = f(y)$, те је $\tilde{f}(x\,\mathrm{Ker}(f)) = \tilde{f}(y\,\mathrm{Ker}(f))$. Функција $\tilde{f}$ је хомоморфизам:

$$\tilde{f}\left((x\,\mathrm{Ker}(f))(y\,\mathrm{Ker}(f))\right) = \tilde{f}((xy)\,\mathrm{Ker}(f)) = f(xy) = f(x) * f(y) =$$

$$= \tilde{f}(x\,\mathrm{Ker}(f)) * \tilde{f}(y\,\mathrm{Ker}(f)).$$

Из дефиниције хомоморфизма $\tilde{f}$, очигледно је да је $\mathrm{Im}(\tilde{f}) = \mathrm{Im}(f)$.

Остаје да се покаже да је $\tilde{f}$ „1–1", тј. да је $\mathrm{Ker}(\tilde{f})$ тривијално. Претпоставимо да $x\,\mathrm{Ker}(f) \in \mathrm{Ker}(\tilde{f})$. То значи да је $\tilde{f}(x\,\mathrm{Ker}(f)) = e_H$. Из дефиниције $\tilde{f}$, следи да $x \in \mathrm{Ker}(f)$, те је $x\,\mathrm{Ker}(f) = \mathrm{Ker}(f)$. □

Наведимо неке примере примене ове теореме.

Пример 90 Ако са $\rho(x, n)$ означимо остатак при дељењу целог броја x природним бројем $n \geq 2$, онда је са $f(x) = \rho(x, n)$ дефинисан хомоморфизам група $f\colon \mathbb{Z} \to \mathbb{Z}_n$, који индукује изоморфизам $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Препоручујемо читаоцима да се сами увере у наведени резултат.

Пример 91 Ако са V означимо подгрупу групе $\mathbb{S}_4$ дату са:

$$V = \{(1), (12)(34), (13)(24), (14)(23)\},$$

онда је $V \triangleleft \mathbb{S}_4$ и $\mathbb{S}_4/V \cong \mathbb{S}_3$.

Већ нам је познато да је V нормална подгрупа (зашто то знамо?). Остаје да се нађе тражени изоморфизам. У ту сврху, ако је $X = \{(12)(34), (13)(24), (14)(23)\}$, дефинишимо хомоморфизам $f : \mathbb{S}_4 \to \mathbb{S}_X$ са:

$$f(\pi)(x) = \pi x \pi^{-1},$$

за $x \in X$. Како је $V \triangleleft \mathbb{S}_4$, јасно је да је $\pi x \pi^{-1} \in V$, за све $x \in X \subset V$. Но, не може бити $\pi x \pi^{-1} = (1)$, јер би тада било $x = (1)$, што није тачно. Дакле, $f(\pi)$ заиста припада $\mathbb{S}_X$. Проверимо да ли је f хомоморфизам:

$$f(\sigma\pi)(x) = (\sigma\pi)x(\sigma\pi)^{-1} = \sigma(\pi x \pi^{-1})\sigma^{-1} = f(\sigma)(\pi x \pi^{-1}) = f(\sigma)(f(\pi)(x)).$$

Добијамо да је $f(\sigma\pi) = f(\sigma) \circ f(\pi)$, те је f заиста хомоморфизам.

Одредимо језгро хомоморфизма f. Пре свега, како је V комутативна, то је $V \subseteq \mathrm{Ker}(f)$ (зашто?). Покажимо да важи и обратно, тј. да је заправо $\mathrm{Ker}(f) = V$. Претпоставимо да $\pi \in \mathrm{Ker}(f)$. То значи да је π пермутација из $\mathbb{S}_4$ за коју важи:

$$\pi(12)(34)\pi^{-1} = (12)(34), \tag{3}$$
$$\pi(13)(24)\pi^{-1} = (13)(24), \tag{4}$$
$$\pi(14)(23)\pi^{-1} = (14)(23). \tag{5}$$

Претпоставимо да је $\pi(1) = 1$. Како је $\pi(12)(34)\pi^{-1} = (\pi(1)\pi(2))(\pi(3)\pi(4))$, из претпоставке да је $\pi(1) = 1$ и једнакости (**??**), следи да је

$$(1\pi(2))(\pi(3)\pi(4)) = (12)(34).$$

Видимо да мора бити $\pi(2) = 2$ и $\pi(3) \in \{3, 4\}$. Уколико је $\pi(3) = 3$, добијамо да је $\pi = (1) \in V$. Претпоставимо да је $\pi(3) = 4$. То значи да је заправо $\pi = (34)$. Но, то би значило да је

$$\pi(13)(24)\pi^{-1} = (\pi(1)\pi(3))(\pi(2)\pi(4)) = (14)(23),$$

што је у супротности са (**??**). Дакле, претпоставка да је $\pi(1) = 1$, доводи до закључка да је π идентична пермутација, те да π припада V. На исти начин се показује да, уколико је $\pi(k) = k$ за било које k, мора бити $\pi = (1)$.

Претпоставимо да π нема фиксну тачку . Сада можемо, без губитка општости, претпоставити да је $\pi(1) = 2$. Из (**??**) добијамо

$$(2\pi(2))(\pi(3)\pi(4)) = (12)(34).$$

Очигледно да мора бити $\pi(2) = 1$ и $\pi(3) \in \{3, 4\}$. Како π нема фиксну тачку, добијамо да је $\pi(3) = 4$ и $\pi(4) = 3$, тј. $\pi = (12)(34) \in V$.

На овај начин смо показали да је $\mathrm{Ker}(f) = V$. Прва теорема о изоморфизмима каже да је тада

$$\mathbb{S}_4/\mathrm{Ker}(f) \cong \mathrm{Im}(f),$$

тј. да је количничка група $\mathbb{S}_4/V$ изоморфна једној подгрупи од $\mathbb{S}_X$. Но, $|\mathbb{S}_4/V| = 24/4 = 6 = |\mathbb{S}_X|$. Закључујемо да мора бити $\mathrm{Im}(f) = \mathbb{S}_X$ и добијамо изоморфизам $\mathbb{S}_4/V \cong \mathbb{S}_X \cong \mathbb{S}_3$. ♣

Наведимо сада теорему, која се доказује применом прве теореме о изоморфизмима група.

Теорема 92 (Факторијел теорема) Нека је H подгрупа групе G коначног индекса n. Тада постоји нормална подгрупа N групе G, која је садржана у подгрупи H и која је и сама коначног индекса. Осим тога: $[G : N] \mid n!$.

Доказ. Нека је $X = G/H$ (дакле, X је скуп свих левих косета подгрупе H у групи G). Дефинишимо хомоморфизам $f: G \to \mathbb{S}_X$ са:

$$f(g)(aH) = (ga)H,$$

за $a \in G$ (елементи у X су леви косети од H, дакле подскупови од G облика aH за неко $a \in G$). На основу прве теореме о изоморфизмима, $G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. Приметимо да важи следеће:

$$\mathrm{Ker}(f) \subseteq H.$$

Наиме, ако $g \in \mathrm{Ker}(f)$, онда мора бити и $f(g)(H) = H$ (H је један од косета, а по претпоставци је $f(g) = id_X$), тј. $gH = H$. Но, из $gH = H$, следи да g припада H. Добили смо да је група $G/\mathrm{Ker}(f)$ изоморфна једној подгрупи групе $\mathbb{S}_X$. С обзиром да је $|X| = n$, добијамо да

$$|G/\mathrm{Ker}(f)| \mid n! \quad . \tag{6}$$

Тиме је доказ завршен – $\mathrm{Ker}(f)$ је тражена нормална подгрупа. □

Последица 93 Нека је p најмањи прост број који дели ред коначне групе G и H подгрупа од G индекса p. Тада је подгрупа H нормална.

Доказ. На основу Факторијел теореме, H садржи нормалну подгрупу N групе G за коју важи: $[G : N] \mid p!$ и $[G : N] \neq 1$ (јер је $N \subseteq H$, а $H \neq G$). Нека је q ма који прост фактор од $[G : N]$. Како $[G : N] \mid p!$, то је или $q = p$, или је $q < p$. Но, $[G : N] \mid |G|$. те и $q \mid |G|$. По претпоставци је p најмањи прост броје који дели ред групе G, па закључујемо да мора бити $q = p$. Дакле, једини прост број који дели $[G : N]$ је p. Стога је $[G : N] = p^s$ за неко $s \geq 1$. Како p^2 не дели $p!$, то мора бити $[G : N] = p = [G : H]$. Закључујемо да је заправо $N = H$, те је H нормална подгрупа од G. □

Пример 94 Свака група реда 15 је циклична.

Кошијева теорема тврди следеће. Ако је G коначна група и p ма који прост број, који дели ред те групе, онда у G постоји елемент реда p. Ову теорему ћемо доказати нешто касније, сада ћемо је применити у овом примеру.

На основу Кошијеве теореме постоји елемент x реда 3 и елемент y реда 5. Подгрупа $H = \langle y \rangle$ је стога индекса 3 и на основу претходног става она је нормална. Стога је

$$xyx^{-1} = y^r \tag{7}$$

за неко $r \in \{1, 2, 3, 4\}$. Уколико је $r = 1$, онда на стандардан начин добијамо да је $G \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$. Покажимо да остале могућности за r нису могуће. Ако (**??**) помножимо слева са x и здесна са x^{-1}, добијамо

$$x^2yx^{-2} = xy^rx^{-1} = (xyx^{-1})^r = (y^r)^r = y^{r^2}. \tag{8}$$

Множењем (**??**) слева са x и здесна са x^{-1} добијамо

$$x^3yx^{-3} = y^{r^3}. \tag{9}$$

Но, с обзиром да је $x^3 = e$ из (**??**) добијамо

$$y = y^{r^3}, \tag{10}$$

тј.

$$y^{r^3-1} = e. \tag{11}$$

Дакле, с обзиром да је $\omega(y) = 5$, мора бити $5 \mid r^3 - 1$. Но, лако се може проверити да 5 не дели ниједан од бројева $2^3 - 1$, $3^3 - 1$, $4^3 - 1$. ♣

Друга и трећа теорема о изоморфизмима укључују у своју формулацију две подгрупе дате групе G.

Теорема 95 (Друга теорема о изоморфизмима) Нека је G група, $H \leq G$ и $K \triangleleft G$. Тада је $HK \leq G$, $H \cap K \triangleleft H$ и

$$HK/K \cong H/H \cap K.$$

Доказ. Пре свега, треба показати да је $HK \leq G$. Како $e \in H \cap K$, то је $e = ee \in HK$, па $HK \neq \emptyset$. Претпоставимо да су x и y елементи из HK. Дакле, постоје елементи $h, h' \in H$ и $k, k' \in K$ такви да је $x = hk$, $y = h'k'$. Тада је

$$x^{-1}y = k^{-1}h^{-1}h'k' = k^{-1}((h')^{-1}h)^{-1}k' =$$

$$= \overbrace{((h')^{-1}h)^{-1}}^{\in H} \underbrace{\overbrace{\left(\underbrace{((h')^{-1}h)}_{\in H}\underbrace{k^{-1}}_{\in K}((h')^{-1}h)^{-1}\right)}^{\in K}}_{\in K} k' \in HK.$$

С обзиром да је $K \triangleleft G$, то је и $K \triangleleft HK$. Дефинишимо функцију $f\colon H \to HK/K$ са: $f(h) = hK$. С обзиром да је

$$f(hh') = (hh')K = (hK)(h'K) = f(h)f(h'),$$

f је хомоморфизам.

Докажимо да је f „на". Нека је xK произвољан елемент из HK/K. Дакле, за неко $h \in H$ и $k \in K$, $x = hk$. Тада је

$$xK = (hk)K = h(kK) = hK = f(h),$$

па је f заиста „на".

Одредимо језгро хомоморфизма f. Узмимо произвољни елемент $h \in H$. Тада $h \in \mathrm{Ker}(f)$ ако и само ако је $f(h) = K$ (K је неутрал у HK/K). С обзиром да је $f(h) = hK$, добијамо да је $h \in \mathrm{Ker}(f)$ ако и само ако $h \in K$, тј. $\mathrm{Ker}(f) = H \cap K$. Прва теорема о изоморфизмима даје: $H/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$, тј. $H/H \cap K \cong HK/K$. Приметимо да $H \cap K \triangleleft H$ следи из чињенице да је $H \cap K$ језгро неког хомоморфизма. □

Пример 96 Нека су $m, n \geq 2$ природни бројеви. Применити другу теорему о изоморфизмима на групе $\mathbb{Z}$, $m\mathbb{Z}$ и $n\mathbb{Z}$.

Друга теорема о изоморфизмима даје

$$(m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} \cong m\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}).$$

Нека је $d = \mathrm{NZD}(m, n)$, а $s = \mathrm{NZS}(m, n)$, тада је

$$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}, \quad m\mathbb{Z} \cap n\mathbb{Z} = s\mathbb{Z}.$$

Дакле,

$$d\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/s\mathbb{Z}.$$

Група $d\mathbb{Z}$ изоморфна је групи $\mathbb{Z}$ при изоморфизму $f\colon \mathbb{Z} \to d\mathbb{Z}$ датом са $f(x) = dx$. Посматрајмо композицију

$$\mathbb{Z} \xrightarrow{f} d\mathbb{Z} \to d\mathbb{Z}/n\mathbb{Z}.$$

Нека је $n = dn'$. Није тешко проверити да је језгро ове композиције заправо подгрупа $n'\mathbb{Z}$. Другим речима, имамо изоморфизам

$$\mathbb{Z}/n'\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z}.$$

Знамо да је $sd = mn$, па је $n' = n/d = s/m$. Заправо је група $m\mathbb{Z}/s\mathbb{Z}$ изоморфна групи $\mathbb{Z}/n'\mathbb{Z}$. ♣

Пример 97 Нека је G коначна група, $H \leq G$, $K \triangleleft G$ и $\mathrm{NZD}(|H|, [G : K]) = 1$. Показати да је $H \subseteq K$.

Нека је $n = |HK/K|$. На основу друге теореме о изоморфизмима, важи изоморфизам $HK/K \cong H/(H \cap K)$. Добијамо да $n \mid |H|$. С друге стране, $HK/K \leq G/K$, те $n \mid |G/K|$. Како је $\mathrm{NZD}(|H|, [G : K]) = 1$, добијамо да је $n = 1$. То значи да је $HK = K$. Како је $H \subseteq HK$ (зашто?), следи да је $H \subseteq K$. ♣

Теорема 98 (Трећа теорема о изоморфизмима) Нека су H и K нормалне подгрупе групе G за које је $H \subseteq K$. Тада је $K/H \triangleleft G/H$ и

$$(G/H)/(K/H) \cong G/K.$$

Доказ. Дефинишимо функцију $f: G/H \to G/K$ са $f(gH) = gK$. Ова функција јесте добро дефинисана пошто из претпоставке да је $gH = g'H$ следи да је $g^{-1}g' \in H$, а како је $H \subseteq K$, то из $g^{-1}g' \in H$ следи да $g^{-1}g' \in K$, па је $gK = g'K$. Очигледно је да је f један епиморфизам. Одредимо језгро од f.

$$gH \in \mathrm{Ker}(f) \text{ акко } gK = K \text{ акко } g \in K.$$

Видимо да је $\mathrm{Ker}(f) = K/H$. Резултат се сада добија применом прве теореме о изоморфизмима. □

Заправо, имамо и нешто прецизнију информацију о подгрупама групе G/H – свака подгрупа $\mathcal{L}$ ове групе је облика L/H за неку подгрупу L групе G, која садржи подгрупу H и $\mathcal{L} \triangleleft G/H$ ако и само ако је $L \triangleleft G$. Размислите како бисте ово доказали.

Пример 99 Нека су природни бројеви $m, n \geq 2$ такви да $m \mid n$. Применити трећу теорему о изоморфизмима на: $\mathbb{Z}$, $m\mathbb{Z}$ и $n\mathbb{Z}$.

Наравно, $n\mathbb{Z}$ је подгрупа од $\mathbb{Z}$ генерисана елементом n. Како $m \mid n$, то је $n\mathbb{Z} \subseteq m\mathbb{Z}$. Дакле, на основу треће теореме о изоморфизмима, добијамо

$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}.$$

Као и у раније наведеном примеру,

$$m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z},$$

где је $d = n/m$. Ми знамо да је свака циклична група реда n изоморфна са $\mathbb{Z}_n$ и $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. Осим тога, за сваки делилац реда цикличне групе, постоји тачно једна подгрупа те групе тог реда. Уколико је G циклична група реда n и $d \mid n$, онда постоји тачно једна подгрупа H групе G, која је реда d и тада је $G/H \cong \mathbb{Z}_m$, где је $m = n/d$. ♣

Коначно генерисане Абелове групе

Подсетимо се диедарске групе:

$$\mathbb{D}_n = \langle\ \sigma, \rho \mid \sigma^2 = \varepsilon, \rho^n = \varepsilon, \sigma\rho = \rho^{n-1}\sigma\ \rangle.$$

Њена абелизација задата је са:

$$\mathbb{D}_n^{\mathrm{Ab}} = \langle\ \sigma, \rho \mid 2\sigma = 0, n\rho = 0, \sigma + \rho = (n-1)\rho + \sigma\ \rangle.$$

Тако добијамо систем једначина

$$\begin{aligned} 2\sigma &= 0 \\ n\rho &= 0 \\ (n-2)\rho &= 0. \end{aligned}$$

Одузимањем последње једначине од претпоследње добијамо систем

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0 \\ (n-2)\rho &= 0. \end{aligned}$$

Природно је разликовати два случаја.

$n = 2k + 1$. Добијамо систем

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0 \\ (2k-1)\rho &= 0. \end{aligned}$$

Уколико од последње једначине одузмемо претпоследњу помножену са $k - 1$ добијамо

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0 \\ \rho &= 0. \end{aligned}$$

Дакле, све се своди на

$$\begin{aligned} 2\sigma &= 0 \\ \rho &= 0. \end{aligned}$$

Према томе ради се о Абеловој групи генерисаној са два генератора σ и ρ, при чему је један од тих генератора (ρ) заправо једнак 0. Тај нам је генератор и непотребан и добијамо Абелову групу са једним генератором σ, који задовољава услов $2\sigma = 0$ и ниједан други (који

није последица овог и аксиома групе). Јасно је да се ради о цикличној групи (пошто је у питању један генератор) реда два (пошто је ред тог генератора 2), те је $\mathbb{D}^{\mathrm{Ab}}_{2k+1} \cong \mathbb{Z}_2$.

$n = 2k$. Овде добијамо систем

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0 \\ (2k-2)\rho &= 0. \end{aligned}$$

Одузимањем од последње једначине претпоследње помножене са $k-1$ добијамо

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0 \\ 0 &= 0, \end{aligned}$$

тј. добијамо систем

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0. \end{aligned}$$

Овде се ради о Абеловој групи генерисаној са два генератора σ и ρ који задовољавају само услове $2\sigma = 0$ и $2\rho = 0$ (и наравно њихове последице, које следе из аксиома групе). Дакле, једини елементи у овој групи су $0, \sigma, \rho, \sigma + \rho$, при чему међу овима нема једнаких и још је $2(\sigma + \rho) = 0$. Закључујемо да се ради о Клајновој групи и добијамо да је $\mathbb{D}^{\mathrm{Ab}}_{2k} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Приметимо да смо у овом разматрању користили, као што је уобичајено за Абелове (комутативне) групе адитивну нотацију, тј. операција у групи означена је са $+$, неутрал са 0, а n-ти степен елемента x означава се са nx.

Наш задатак је да покажемо да је *свака коначно генерисана Абелова група* изоморфна директном производу цикличних група. Важна је претпоставка да се ради о коначно генерисаној Абеловој групи, пошто група $(\mathbb{Q}, +)$ није изоморфна директном производу цикличних група, али она нема коначан скуп генератора (размислите како бисте показали да она није изоморфна директном производу цикличних, можда ће вам наставак лекције помоћи у томе).

Уведимо још неке ознаке за Абелове групе. Уколико је A Абелова група, а B, C њене подгрупе, онда је

$$B + C := \{b + c : b \in B, c \in C\}.$$

Јасно је да је ово подгрупа групе A и то је заправо најмања подгрупа групе A, која садржи B и C као своје подгрупе (докажите то!). Наравно да је називамо *сума подгрупа B и C*. Уколико је $B \cap C = \{0\}$, онда

је сума $B+C$ директна и пишемо $B \oplus C$ (присетите се суме векторских простора из линеарне алгебре). У случају директне суме, сваки елемент x из те суме може се *на јединствен начин* приказати у облику $x = b + c$, где b припада подгрупи B, а c подгрупи C. Наиме, како је у питању сума подгрупа, јасно је да је сваки елемент тог облика. Докажимо јединственост. Уколико је

$$x = b + c, \quad x = b_1 + c_1,$$

где $b, b_1 \in B$, $c, c_1 \in C$ онда је $b - b_1 = c_1 - c$, но овај елемент припада и подгрупи B и подгрупи C, а како је њихов пресек тривијалан то мора бити $b - b_1 = 0$ и $c_1 - c = 0$, тј. $b = b_1$ и $c = c_1$, те је приказ јединствен.

Сва ова дискусија о директној суми две подгрупе заправо показује да важи следећи изоморфизам

$$B \times C \cong B \oplus C.$$

Наиме, лако се провери да је са $f(b, c) = b + c$ задат један изоморфизам $f: B \times C \to B \oplus C$.

Као и у случају векторских простора и овде се може увести директна сума коначно много подгрупа Абелове групе (подсетите се услова) и показати да је $A_1 \times \cdots \times A_n \cong A_1 \oplus \cdots \oplus A_n$. Урадите то за вежбу.

Дакле, ми се у овој лекцији бавимо коначно генерисаним Абеловим групама. Абелова група A је коначно генерисана уколико постоји коначан подскуп $\{x_1, \ldots, x_s\} \subseteq A$ такав да важи:

$$A = \{m_1 x_1 + \cdots + m_s x_s : m_i \in \mathbb{Z}, i = \overline{1, s}\}$$

(подсетите се дефиниције подгрупе дефинисане неким скупом уз чињеницу да је група A Абелова). Другим речима,

$$A = \langle x_1 \rangle + \cdots + \langle x_s \rangle.$$

Према томе, свака коначно генерисана Абелова група је сума коначно много цикличних група. Наш задатак је у томе да докажемо да је свака коначно генерисана Абелова група заправо директна сума коначно много цикличних група (те је према претходним напоменама изоморфна директном производу цикличних група).

Уведимо неке неопходне појмове.

Ако је n најмањи број за који дата група A има систем од n генератора (систем од n генератора је уређена n-торка елемената групе који генеришу целу групу) и ако је $[x_1, \ldots, x_n]$ један такав систем генератора, онда за њега кажемо да је један минималан систем генератора. Важно је приметити да важи следеће.

> Ако је $[x_1, x_2, \ldots, x_n]$ минималан систем генератора и $q_2, \ldots, q_n$ ма који цели бројеви, онда је и $[x_1 + q_2 x_2 + \cdots q_n x_n, x_2, \ldots, x_n]$ један минималан систем генератора.

У ову чињеницу, није се тешко уверити. Само треба показати да је и новодобијени систем такође систем генератора. За то је довољно да се покаже да се сваки од елемената $x_1, \ldots, x_n$ може изразити преко ових генератора, а једино што ту заиста треба проверити је да је x_1 такав. Но, то је јасно:

$$x_1 = (x_1 + q_2x_2 + \cdots q_nx_n) - q_2x_2 - \cdots - q_nx_n.$$

Дефиниција 100 Нека је $[x_1, \ldots, x_n]$ систем генератора. Формула облика

$$m_1x_1 + \cdots + m_nx_n = 0,$$

где су $m_1, \ldots, m_n \in \mathbb{Z}$, зове се релација међу генераторима. Релација је нетривијална уколико је бар један од коефицијената m_i различит од нуле.

Наравно да би ова дефиниција требало да нас подсети на појам линеарне зависности међу векторима у векторском простору. Како радимо са Абеловим групама, овде имамо целобројне коефицијенте.

Дефиниција 101 Коначно генерисана Абелова група је слободна уколико она има систем генератора међу којима нема нетривијалних релација.

Став 102 Свака коначно генерисана слободна Абелова група изоморфна је тачно једној групи облика $\mathbb{Z}^n$ за неко $n \geq 1$.

Наравно, са $\mathbb{Z}^n$ означен је директан производ од n група $\mathbb{Z}$.

Доказ. Нека је A нека коначно генерисана слободна Абелова група и $[x_1, \ldots, x_n]$ један систем генератора међу којима нема нетривијалних релација. Дефинишимо функцију $f\colon \mathbb{Z}^n \to A$ са:

$$f(m_1, \ldots, m_n) = m_1x_1 + \cdots + m_nx_n.$$

Није тешко уверити се да је f један изоморфизам. Пре свега, јасно је да је f „на", пошто је $[x_1, \ldots, x_n]$ систем генератора, те је заиста сваки елемент у групи траженог облика. Осим тога, f је и „1–1". Наиме, ако је $f(m_1, \ldots, m_n) = f(p_1, \ldots, p_n)$ то значи да је

$$m_1x_1 + \cdots + m_nx_n = p_1x_1 + \cdots + p_nx_n.$$

Следи да је

$$(m_1 - p_1)x_1 + \cdots + (m_n - p_n)x_n = 0.$$

Како међу генераторима $x_1, \ldots, x_n$, по претпоставци, нема нетривијалних релација, закључујемо да је $m_1 - p_1 = \cdots = m_n - p_n = 0$, те је f заиста „1–1". Оставља се за (врло лаку) вежбу доказ чињенице да се f слаже са операцијама.

Дакле, доказали смо да је свака коначно генерисана слободна Абелова група изоморфна некој од група $\mathbb{Z}^n$. Остаје да докажемо јединственост, тј. да из $\mathbb{Z}^m \cong \mathbb{Z}^n$ следи да је $m = n$.

Претпоставимо, стога, да је $\mathbb{Z}^m \cong \mathbb{Z}^n$ и да је $m \leq n$. Искористићемо знање линеарне алгебре. Наиме, у групи $\mathbb{Z}^n$ постоје канонски генератори

$$\begin{array}{rcl} e_1 & = & (1,0,\ldots,0) \\ e_2 & = & (0,1,\ldots,0) \\ \vdots & \vdots & \vdots \quad \vdots \quad \vdots \quad \vdots \\ e_n & = & (0,0,\ldots,1) \end{array}$$

n-димензионалног векторског простора $\mathbb{R}^n$. Нека је $h\colon \mathbb{Z}^m \to \mathbb{Z}^n$ један изоморфизам. Генератори групе $\mathbb{Z}^m$ су наравно

$$\begin{array}{rcl} e'_1 & = & (1,0,\ldots,0) \\ e'_2 & = & (0,1,\ldots,0) \\ \vdots & \vdots & \vdots \quad \vdots \quad \vdots \quad \vdots \\ e'_m & = & (0,0,\ldots,1) \end{array}$$

и има их m. За сваки генератор e_i групе $\mathbb{Z}^n$ постоје цели бројеви $a_{i1},\ldots,a_{im}$ такви да је

$$e_i = h(a_{i1}e'_1 + \cdots + a_{im}e'_m) = a_{i1}h(e'_1) + \cdots + a_{im}h(e'_m).$$

Из овога следи, ако сада посматрамо реални векторски простор $\mathbb{R}^n$, да је сваки од вектора базе тог простора добијен као линерна комбинација m вектора: $h(e'_1),\ldots,h(e'_m)$, те ти вектори чине једну генератрису тог простора. Но, ми знамо да n-димензионални векторски простор не може бити генерисан са мање од n вектора. Другим речима, мора бити $m \geq n$, те закључујемо да је $m = n$ што и завршава тражени доказ. □

Докажимо најпре два става, који су од општег значаја, а биће коришћени и у даљем излагању.

Став 103 Нека су G_1, G_2 групе и $H_1 \triangleleft G_1$, $H_2 \triangleleft G_2$. Тада је $H_1 \times H_2 \triangleleft G_1 \times G_2$ и

$$G_1 \times G_2 / H_1 \times H_2 \cong G_1/H_1 \times G_2/H_2.$$

Доказ. Јасно је да $H_1 \times H_2 \neq \emptyset$, јер $(e_1, e_2) \in H_1 \times H_2$ (наравно, са e_i означен је неутрал у групи G_i). Ако $(h_1,h_2),(h'_1,h'_2) \in H_1 \times H_2$, онда је и $(h_1,h_2)^{-1}(h'_1,h'_2) = (h_1^{-1},h_2^{-1})(h'_1,h'_2) = (h_1^{-1}h'_1, h_2^{-1}h'_2) \in H_1 \times H_2$, те је, заиста, $H_1 \times H_2$ подгрупа од $G_1 \times G_2$. Ова подгрупа је и нормална, јер из $(h_1,h_2) \in H_1 \times H_2$ и $(g_1,g_2) \in G_1 \times G_2$ следи да је

$$(g_1,g_2)(h_1,h_2)(g_1,g_2)^{-1} = (g_1,g_2)(h_1,h_2)(g_1^{-1},g_2^{-1}) = (g_1h_1g_1^{-1}, g_2h_2g_2^{-1}),$$

а овај елемент припада $H_1 \times H_2$, јер су подгрупе H_1 и H_2 нормалне.

Дефинишимо $f: G_1/H_1 \times G_2/H_2 \to G_1 \times G_2/H_1 \times H_2$ са:

$$f(g_1H_1, g_2H_2) = (g_1, g_2)H_1 \times H_2.$$

Проверимо најпре добру дефинисаност f.

$$\begin{aligned} & (g_1H_1, g_2H_2) = (g_1'H_1, g_2'H_2) \\ \Rightarrow \quad & g_1H_1 = g_1'H_1, g_2H_2 = g_2'H_2 \\ \Rightarrow \quad & g_1^{-1}g_1' \in H_1, g_2^{-1}g_2' \in H_2 \\ \Rightarrow \quad & (g_1^{-1}g_1', g_2^{-1}g_2') \in H_1 \times H_2 \\ \Rightarrow \quad & (g_1, g_2)^{-1}(g_1', g_2') \in H_1 \times H_2 \\ \Rightarrow \quad & (g_1, g_2)H_1 \times H_2 = (g_1', g_2')H_1 \times H_2. \end{aligned}$$

На сличан начин се проверава да је f „1–1".

$$\begin{aligned} & f(g_1H_1, g_2H_2) = f(g_1'H_1, g_2'H_2) \\ \Rightarrow \quad & (g_1, g_2)H_1 \times H_2 = (g_1', g_2')H_1 \times H_2 \\ \Rightarrow \quad & (g_1, g_2)^{-1}(g_1', g_2') \in H_1 \times H_2 \\ \Rightarrow \quad & (g_1^{-1}g_1', g_2^{-1}g_2') \in H_1 \times H_2 \\ \Rightarrow \quad & g_1^{-1}g_1' \in H_1, g_2^{-1}g_2' \in H_2 \\ \Rightarrow \quad & g_1H_1 = g_1'H_1, g_2H_2 = g_2'H_2. \end{aligned}$$

Како је f очигледно „на" (зашто је f „на"?), то остаје да се провери да се f слаже са операцијама.

$$\begin{aligned} f((g_1H_1, g_2H_2)(g_1'H_1, g_2'H_2) &= f((g_1g_1')H_1, (g_2g_2')H_2) \\ &= (g_1g_1', g_2g_2')H_1 \times H_2 \\ &= ((g_1, g_2)(g_1', g_2'))H_1 \times H_2 \\ &= (g_1, g_2)H_1 \times H_2 \cdot (g_1', g_2')H_1 \times H_2 \\ &= f(g_1H_1, g_2H_2)f(g_1'H_1', g_2'H_2). \end{aligned}$$

□

Дефинишимо једну важну подгрупу сваке Абелове групе. То је торзиона подгрупа.

Дефиниција 104 Нека је A Абелова група. Са $T(A)$ означавамо скуп свих елемената из A који су коначног реда.

Покажимо да је $T(A)$ заиста подгрупа од A (у односу на рестрикцију операције са A). Наиме, $0 \in T(A)$. Осим тога, ако $x, y \in T(A)$, то значи да постоје $m, n > 0$ за које је $mx = 0$ и $ny = 0$. Но, тада је $mn(x-y) = mnx - mny = nmx - mny = n0 - m0 = 0$, те је и елемент $x-y$ коначног реда.

Став 105 Нека су A и B изоморфне Абелове групе. Тада је и $T(A) \cong T(B)$ и $A/T(A) \cong B/T(B)$.

Доказ. Нека је $f\colon A \to B$ изоморфизам. Покажимо да је $f[T(A)] = T(B)$, из чега ће следити да рестрикција f на $T(A)$ успоставља први тражени изоморфизам. Но, како је f изоморфизам, то за сваки елемент $x \in A$ важи: $\omega(x) = \omega(f(x))$ ово показује да се елемент коначног реда слика у елемент коначног реда, тј. да је $f[T(A)] \subseteq T(B)$. Нека је $y \in T(B)$. Како је f „на", то постоји $x \in A$ за који је $f(x) = y$. Но, како је $\omega(y) = \omega(f(x)) = \omega(x)$, то је и x коначног реда, тј. $x \in T(A)$. Закључујемо да је заиста $f[T(A)] = T(B)$.

Докажимо да је и $A/T(A) \cong B/T(B)$. Дефинишемо $\tilde{f}\colon A/T(A) \to B/T(B)$ са: $\tilde{f}(a+T(A)) := f(a)+T(B)$. Функција $\tilde{f}$ јесте добро дефинисана. Наиме, ако је $a + T(A) = a' + T(A)$, то значи да је $a - a' \in T(A)$. Но, тада је и $f(a) - f(a') = f(a-a') \in f[T(A)] = T(B)$, те је $f(a)+T(B) = f(a') + T(B)$.

Покажимо да је $\tilde{f}$ „1–1". Нека је $\tilde{f}(a+T(A)) = \tilde{f}(a'+T(A))$. То значи да је $f(a) + T(B) = f(a') + T(B)$, те је $f(a - a') = f(a) - f(a') \in T(B)$, те је и елемент $a - a'$ коначног реда (зашто?), тј. $a - a' \in T(A)$, па следи да је $a + T(A) = a' + T(A)$.

Нека је $b+T(B)$ произвољан елемент из $B/T(B)$. Како је f „на", то постоји $a \in A$ тако да је $b = f(a)$. Но, тада је $b + T(B) = f(a) + T(B) = \tilde{f}(a + T(A))$. Закључујемо да је $\tilde{f}$ и „на".

Остаје да се покаже да се $\tilde{f}$ слаже са операцијама.

$$\begin{aligned}
\tilde{f}((a + T(A)) + (a' + T(A))) &= \tilde{f}((a + a') + T(A)) \\
&= f(a + a') + T(B) \\
&= (f(a) + f(a')) + T(B) \\
&= (f(a) + T(B)) + (f(a') + T(B)) \\
&= \tilde{f}(a + T(A)) + \tilde{f}(a' + T(A)).
\end{aligned}$$

□

Следећи једноставан став је веома користан.

Став 106 Нека је $q \in \mathbb{Z} \setminus \{0\}$ и $n \geq 2$. Тада је број решења једначине $qx = 0$ у групи $\mathbb{Z}_n$ једнак $\mathrm{NZD}(q, n)$.

Доказ. Нека је $x \in Z_n = \{0, 1, \ldots, n-1\}$. Тада је

$$qx = 0 \text{ у групи } \mathbb{Z}_n \textbf{ акко } n \mid qx \text{ у } \mathbb{Z}.$$

Нека је $d = \mathrm{NZD}(q, n)$. То значи да је $q = dq_1$ и $n = dn_1$, при чему је $\mathrm{NZD}(q_1, n_1) = 1$. Како $n \mid qx$, то $dn_1 \mid dq_1x$, па $n_1 \mid q_1x$. Како су n_1 и q_1 узајамно прости, добијамо да $n_1 \mid x$. Дакле, за $x \in \{0, 1, \ldots, n-1\}$ важи: $qx = 0$ у групи $\mathbb{Z}_n$ ако и само ако је $x \in \{0, n_1, 2n_1, \ldots, (d-1)n_1\}$. Закључујемо да једначина $qx = 0$ у групи $\mathbb{Z}_n$ заиста има $d = \mathrm{NZD}(q, n)$ решења. □

Последица 107 Број решења једначине $qx = 0$ у групи $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ једнак је $\mathrm{NZD}(q, n_1)\mathrm{NZD}(q, n_2) \cdots \mathrm{NZD}(q, n_k)$.

Доказ. Овај резултат непосредно следи из претходног става. Наиме, ако је $x = (x_1, x_2, \ldots, x_k) \in Z_{n_1} \times Z_{n_2} \times \cdots Z_{n_k}$, то је $qx = 0$ ако и само ако је за све $i = \overline{1,k}$: $qx_i = 0$. С обзиром да је, према претходном ставу, број решења једначине $qx_i = 0$ у групи $\mathbb{Z}_{n_i}$ једнак $\mathrm{NZD}(q, n_i)$, то тражени резултат следи. □

Урадимо један пример примене претходно доказаног.

Пример 108 У групи $\mathbb{Z}_5 \times \mathbb{Z}_{10} \times \mathbb{Z}_{60}$ одредити број елемената реда 3, 6 и 12.

Означимо нашу групу са A. Тада је број елемената реда 3 у A за један мањи од броја решења једначине $3x = 0$ у A (пошто је 0 такође једно решење ове једначине, а то је неутрал, те није елемент реда 3). Дакле, број елемената реда 3 у овој групи једнак је:

$$\mathrm{NZD}(3,5)\mathrm{NZD}(3,10)\mathrm{NZD}(3,60) - 1 = 1 \cdot 1 \cdot 3 - 1 = 2.$$

Нешто је сложеније одређивање елемената реда 6. Наиме сваки елемент реда 6 јесте решење једначине $6x = 0$ у A, али су и елементи реда 2 и реда 3 такође решења ове једначине. Заправо:

$$\{x \in A : \omega(x) = 6\} = \{x \in A : 6x = 0, 2x \neq 0, 3x \neq 0\}.$$

Дакле, треба одредити број елемената у скупу

$$\{x \in A : 6x = 0\} \setminus (\underbrace{\{x \in A : 2x = 0\}}_{B} \cup \underbrace{\{x \in A : 3x = 0\}}_{C}).$$

По добро познатој формули: $|B \cup C| = |B| + |C| - |B \cap C|$. Но,

$$x \in B \cap C \text{ акко } 2x = 0 \text{ и } 3x = 0.$$

Закључујемо да је $B \cap C = \{0\}$. Број елемената у B је, према претходној последици, једнак $\mathrm{NZD}(2,5)\mathrm{NZD}(2,10)\mathrm{NZD}(2,60) = 1 \cdot 2 \cdot 2 = 4$. На исти начин се добије да је $|C| = 1 \cdot 1 \cdot 3 = 3$, док је $|\{x \in A : 6x = 0\}| = 1 \cdot 2 \cdot 6 = 12$. Добијамо да је број елемената реда 6 у групи A једнак $12 - (4 + 3 - 1) = 6$.

Најсложеније је одређивање броја елемената реда 12. Наиме,

$$\{x \in A : \omega(x) = 12\} = \{x \in A : 12x = 0 \wedge (\forall d)(1 \leq d < 12 \Rightarrow dx \neq 0)\}.$$

Није тешко уверити се да се ово може поједноставити, тј. да је

$$\{x \in A : (\exists d)(1 \leq d < 12 \wedge dx = 0)\} = \underbrace{\{x \in A : 4x = 0\}}_{D} \cup \underbrace{\{x \in A : 6x = 0\}}_{E}.$$

Приметимо да је $D \cap E = \{x \in A : 6x = 0, 4x = 0\} = \{x \in A : 2x = 0\}$. Како је

$$\begin{aligned}
|\{x \in A : 12x = 0\}| &= \mathrm{NZD}(12,5)\mathrm{NZD}(12,10)\mathrm{NZD}(12,60) = 1 \cdot 2 \cdot 12 = 24 \\
|\{x \in A : 4x = 0\}| &= \mathrm{NZD}(4,5)\mathrm{NZD}(4,10)\mathrm{NZD}(4,60) = 1 \cdot 2 \cdot 4 = 8 \\
|\{x \in A : 6x = 0\}| &= \mathrm{NZD}(6,5)\mathrm{NZD}(6,10)\mathrm{NZD}(6,60) = 1 \cdot 2 \cdot 6 = 12 \\
|\{x \in A : 2x = 0\}| &= \mathrm{NZD}(2,5)\mathrm{NZD}(2,10)\mathrm{NZD}(2,60) = 1 \cdot 2 \cdot 2 = 4,
\end{aligned}$$

то је број елемената реда 12 у групи A једнак: $24-(8+12-4)=8$. ♣

Користећи до сада урађено, можемо доказати следећи став.

Став 109 Нека су $k,l,s,t\geq 0$ и $d_1,\ldots,d_k$, $r_1,\ldots,r_l$ природни бројеви такви да је $d_1>1$, $r_1>1$, $d_i \mid d_{i+1}$, за $i=\overline{1,k-1}$ и $r_j \mid r_{j+1}$, за $j=\overline{1,l-1}$. Тада из

$$\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_2}\times\cdots\times\mathbb{Z}_{d_k}\times\mathbb{Z}^s\cong\mathbb{Z}_{r_1}\times\mathbb{Z}_{r_2}\times\cdots\times\mathbb{Z}_{r_l}\times\mathbb{Z}^t$$

следи: $s=t$, $k=l$ и $d_i=r_i$ за све $i=\overline{1,k}$.

Доказ. У доказу ћемо користити став **??**. У ту сврху, одредимо торзионе подгрупе наведених група. Важи следеће:

$$T(\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_2}\times\cdots\times\mathbb{Z}_{d_k}\times\mathbb{Z}^s)=\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_2}\times\cdots\times\mathbb{Z}_{d_k}\times\{0\}^s.$$

Наиме, нека је $x=(x_1,\ldots,x_k,y_1,\ldots,y_s)\in\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_2}\times\cdots\times\mathbb{Z}_{d_k}\times\mathbb{Z}^s$. Уколико је за бар једно j_0: $y_{j_0}\neq 0$, онда за ма које $n\geq 1$ важи: $n(x_1,\ldots,x_k,y_1,\ldots,y_s)=(nx_1,\ldots,nx_k,ny_1,\ldots,ny_s)\neq(0,\ldots,0,0,\ldots,0)$, јер $ny_{j_0}\neq 0$. Дакле, такав елемент не може бити коначног реда. С друге стране, јасно је да је $d_k(x_1,\ldots,x_k,0,\ldots,0)=(0,\ldots,0,0,\ldots,0)$ те закључујемо да је торзиона група заиста горенаведена подгрупа. Из става **??** следи да су за дате групе изоморфне њихове торзионе подгрупе и одговарајуће количничке групе, што, уз примену става **??** (како се тачно тај став примењује?) следи да је

$$\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_2}\times\cdots\times\mathbb{Z}_{d_k}\cong\mathbb{Z}_{r_1}\times\mathbb{Z}_{r_2}\times\cdots\times\mathbb{Z}_{r_l}\text{ и }\mathbb{Z}^s\cong\mathbb{Z}^t.$$

На основу става **??** добијамо да је $s=t$. Концентришимо се сада на изоморфизам

$$\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_2}\times\cdots\times\mathbb{Z}_{d_k}\cong\mathbb{Z}_{r_1}\times\mathbb{Z}_{r_2}\times\cdots\times\mathbb{Z}_{r_l}.$$

Претпоставимо, на пример, да је $k\geq l$. Ако са L означимо групу са леве стране, а са D групу са десне стране, посматрајмо број решења једначине $d_1x=0$ у овим групама. Како су оне изоморфне, то постоји и бијекција између скупа решења ових једначина (уверите се у то!). Но, број решења ове једначине у групи L једнак је

$$\mathrm{NZD}(d_1,d_1)\mathrm{NZD}(d_1,d_2)\cdots\mathrm{NZD}(d_1,d_k)=d_1\cdot d_1\cdots d_1=d_1^k,$$

с обзиром на чињеницу да $d_1 \mid d_i$ за све $i\geq 1$. У групи D, број решења ове једначине једнак је

$$\mathrm{NZD}(d_1,r_1)\mathrm{NZD}(d_1,r_2)\cdots\mathrm{NZD}(d_1,r_l),$$

при чему је сваки од фактора у производу не већи од d_1. С обзиром да је овај производ једнак d_1^k и да је $k\geq l$, мора бити $k=l$ и морају сви фактори у овом производу бити једнаки d_1. Одавде следи да $d_1 \mid r_1$. Уколико бисмо сада посматрали број решења једначине $r_1x=0$ у овим

групама, на исти начин бисмо добили да $r_1 \mid d_1$. Закључујемо да смо добили да је $k = l$ и $d_1 = r_1$.

Посматрајмо сада број решења једначине $d_2 x = 0$ у овим групама. Број решења ове једначине у групи L је $d_1 d_2^{k-1}$, док је у групи D тај број $d_1 s_2 \dots s_k$ при чему је $s_i \leq d_i$ за све $i \geq 2$. Добијамо да је $d_1 d_2^{k-1} = d_1 s_2 \dots s_k$. Скраћивањем са d_1 и коришћењем чињенице да је $s_i \leq d_i$, добијамо да мора бити $s_i = d_i$ за све $i \geq 2$. То посебно значи да $d_2 \mid r_2$. На исти начин као и пре, посматрањем броја решења једначине $r_2 x = 0$ у овим групама, добијамо да $r_2 \mid d_2$, па мора бити $d_2 = r_2$. Настављањем овог поступка добијамо да је за све $i = \overline{1,k}$: $d_i = r_i$, што је и требало доказати. □

Пређимо сада на нашу главну теорему.

Теорема 110 Нека је A коначно генерисана Абелова група. Тада је A изоморфна тачно једној групи облика $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^l$, где је $k \geq 0$, $l \geq 0$, $d_1 > 1$ и $d_i \mid d_{i+1}$ за $i = \overline{1, k-1}$.

Доказ. Из претходних резултата следи јединственост групе наведеног облика. Докажимо сада егзистенцију.

Изводимо доказ индукцијом по минималном броју генератора. Означимо тај минималан број генератора са n. Наравно, група генерисана празним скупом генератора је тривијална група $\{0\}$. Према томе, $n \geq 1$.

$n = 1$. У овом случају је све јасно – ради се о цикличној групи и ми знамо да је свака циклична група изоморфна или групи $\mathbb{Z}$, или групи $\mathbb{Z}_d$ за неко $d > 1$.

Претпоставимо да је $n > 1$ и да је тврђење тачно за све групе са мање од n генератора. Имамо две могућности.
1. Међу n генератора групе A нема нетривијалних релација. На основу претходног става закључујемо да је A изоморфна групи $\mathbb{Z}^n$.
2. Међу генераторима групе A има нетривијалних релација. Означимо са $d_1 > 0$ најмањи цео број за који постоји систем генератора $[x_1, \dots, x_n]$ групе A, за који важи релација

$$d_1 x_1 + m_2 x_2 + \cdots + m_n x_n = 0 \tag{12}$$

за неке целе бројеве $m_2, \dots, m_n$. Тврдимо да важи следеће.

> Ако је $[y_1, y_2, \dots, y_n]$ ма који систем генератора за који важи $d_1 y_1 + r_2 y_2 + \cdots + r_n y_n = 0$, за неке целе бројеве $r_2, \dots, r_n$, онда $d_1 \mid r_i$ за све $i = \overline{2, n}$.

У супротном, претпоставимо да ово није тачно за неке целе r_i и нека, на пример, d_1 не дели r_2. То значи да је $r_2 = q d_1 + s$, при чему је $0 < s < r_2$. Дакле,

$$d_1 y_1 + (q d_1 + s) y_2 + \cdots + r_n y_n = 0,$$

па је и

$$d_1(y_1 + qy_2) + sy_2 + \cdots + r_n y_n = 0.$$

Према ранијој напомени, $[y_1+qy_2, y_2, \ldots, y_n]$ је такође један систем генератора, а то је онда, наравно, и $[y_2, y_1 + qy_2, \ldots, y_n]$, но за тај систем генератора постоји (нетривијална) релација

$$sy_2 + d_1(y_1 + qy_2) + \cdots + r_n y_n = 0,$$

при чему је $0 < s < d_1$. То противречи дефиниционом својству коефицијента d_1 те на тај начин добијамо контрадикцију.

Вратимо се на релацију (**??**). Према доказаном, $d_1 \mid m_2, \ldots, d_1 \mid m_n$. Дакле, за неке целе бројеве q_i је $m_i = d_1 q_i$ за $i = \overline{2,n}$. Релација (**??**) своди се на

$$d_1 x_1 + d_1 q_2 x_2 + \cdots + d_1 q_n x_n = 0,$$

тј. на

$$d_1(x_1 + q_2 x_2 + \cdots + q_n x_n) = 0.$$

Добијамо нови систем генератора $[z_1, x_2, \ldots, x_n]$ (где је $z_1 = x_1 + q_2 x_2 + \cdots + q_n x_n$) код кога је $d_1 z_1 = 0$. Уколико би d_1 био једнак 1, онда би и наша група имала мање од n генератора, а то противречи претпоставци. Стога је $d_1 > 1$. Посматрајмо две подгрупе групе A:

$$A_1 = \langle z_1 \rangle, \quad B_1 = \langle x_2, \ldots, x_n \rangle.$$

Јасно је да је $A_1 \cong \mathbb{Z}_{d_1}$ (зашто је то јасно?). Приметимо да је $A_1 + B_1 = A$. Докажимо да је ова сума заправо директна, тј. да је $A_1 \cap B_1 = \{0\}$. У супротном, постоји нетривијалан елемент у овом пресеку, тј. за неко $s_1 \in \{1, \ldots, d_1 - 1\}$ и неке целе $s_2, \ldots, s_n$ важи:

$$s_1 z_1 = s_2 x_2 + \cdots + s_n x_n.$$

Добијамо да је

$$s_1 z_1 + (-s_2) x_2 + \cdots + (-s_n) x_n = 0,$$

при чему је $0 < s_1 < d_1$. То је, наравно, у контрадикцији са дефиниционим својством броја d_1, те тако нешто није могуће и пресек ових подгрупа је тривијалан. Добили смо да је

$$A = A_1 \oplus B_1 \cong A_1 \times B_1 \cong \mathbb{Z}_{d_1} \times B_1.$$

Абелова група B_1 има мање од n генератора, па је по индуктивној хипотези изоморфна директном производу цикличних група (као што је наведено у формулацији теореме). Ако је она изоморфна групи Z^{n-1}, доказ је завршен. У супротном, појављују се и коначне цикличне групе у производу:

$$B_1 \cong \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^l,$$

при чему је $k \geq 2$ и $d_i \mid d_{i+1}$ за $i = \overline{2, k-1}$. Тврдимо да $d_1 \mid d_2$. У супротном, група A има систем генератора $[z_1, z_2, \ldots, z_n]$ (где су генератори z_i, за $i \geq 2$, генератори подгрупа које одговарају преосталим факторима у директном производу), при чему је $d_2 z_2 = 0$. Но, тада је $d_1 z_1 + d_2 z_2 + 0 z_3 + \cdots + 0 z_n = 0$, те на основу раније доказаног следи да $d_1 \mid d_2$ (на основу чега ово следи?). Тиме је завршен доказ да је свака коначно генерисана Абелова група изоморфна директном производу цикличних група траженог облика. □

Групу наведеног облика, изоморфну групи A, зовемо и нормална форма те групе, а бројеве d_i инваријантним делитељима. Осим ове форме, постоји и елементарна форма те групе. Наиме, коришћењем чињенице да важи изоморфизам $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, уколико су m и n узајамно прости, добијамо да се свака коначно генерисана Абелова група може представити у облику производа цикличних група, при чему је свака коначна циклична група, која се појављује у том производу, реда једнаког степену неког простог броја. На пример, за групу $\mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{60}$ важи изоморфизам

$$\mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{60} \cong \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \times (\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

и тако је добијена елементарна форма те групе.

На самом почетку излагања о коначно генерисаним Абеловим групама, било је речи о примеру Абелизације диедарске групе, која је била задата помоћу генератора и релација међу тим генераторима. Продискутујмо сада општи случај.

Шта заправо значи када кажемо да је група задата генераторима и релацијама? Нека је, на пример, група A задата генераторима $x_1, \ldots, x_n$ и релацијама

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots &\quad . \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0. \end{aligned} \tag{13}$$

Ако је $r_j = a_{j1}x_1 + a_{j2}x_2 + \cdots + a_{jn}x_n$, онда је заправо група A изоморфна количничкој групи

$$F_n / \langle r_1, \ldots, r_m \rangle,$$

где је са F_n означена слободна Абелова група са n генератора $x_1, \ldots, x_n$. Наиме, знамо да у слободној Абеловој групи са n генератора $x_1, \ldots, x_n$ (где је n минималан број генератора) нема релација међу генераторима. Да бисмо ми увели неке релације, ми ту групи „сечемо" по елементима који дефинишу релације (тако да ти елементи постају неутрал у количничкој групи), односно са групом генерисаном тим елементима.

Погледајмо како то изгледа у посебно једноставном случају када су релације облика

$$\begin{aligned} d_1 x_1 &= 0 \\ d_2 x_2 &= 0 \\ \cdots & \quad . \\ d_k x_k &= 0. \end{aligned}$$

Тада је $A \cong \langle x_1, \ldots, x_k, \ldots, x_n \rangle / \langle d_1 x_1, \ldots, d_k x_k \rangle$. Но, с обзиром да су $x_1, \ldots, x_n$ слободни генератори групе $\langle x_1, \ldots, x_n \rangle$, тј. генератори међу којима нема релација, то је $\langle x_1, \ldots, x_n \rangle = \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle$, те је

$$\begin{aligned} A &\cong \langle x_1 \rangle \oplus \cdots \oplus \langle x_k \rangle \oplus \cdots \oplus \langle x_n \rangle / (\langle d_1 x_1 \rangle \oplus \cdots \oplus \langle d_k x_k \rangle) \\ &\cong \langle x_1 \rangle \times \cdots \times \langle x_k \rangle \times \cdots \times \langle x_n \rangle / (\langle d_1 x_1 \rangle \times \cdots \times \langle d_k x_k \rangle) \\ &\cong \langle x_1 \rangle \times \cdots \times \langle x_k \rangle \times \langle x_{k+1} \rangle \times \cdots \times \langle x_n \rangle / \langle d_1 x_1 \rangle \times \cdots \times \langle d_k x_k \rangle \times \{0\} \times \cdots \times \{0\} \\ &\cong \langle x_1 \rangle / \langle d_1 x_1 \rangle \times \cdots \times \langle x_k \rangle / \langle d_k x_k \rangle \times \langle x_{k+1} \rangle / \{0\} \times \cdots \times \langle x_n \rangle / \{0\}. \end{aligned}$$

С обзиром да је $\langle x_i \rangle / \langle d_i x_i \rangle \cong \mathbb{Z}_{d_i}$ и да је $\langle x_i \rangle / \{0\} \cong \mathbb{Z}$, то добијамо да је $A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$.

Поставља се питање да ли можемо трансформисати почетне релације међу генераторима у овако једноставне релације међу (можда неким другим генераторима), пошто бисмо на тај начин очигледно могли да добијемо нормалну форму дате групе. Одговор је да је то могуће урадити.

Преформулишимо најпре наш проблем на проблем у вези матрица над прстеном целих бројева. Релације (**??**) очигледно се могу и овако записати:

$$AX = \mathbf{0},$$

где је A матрица $A = [a_{ij}]_{m \times n} \in M_{mn}(\mathbb{Z})$, $X = [x_1, \ldots, x_n]^T$ и $\mathbf{0} = [0, \ldots, 0]^T$. (Додуше, овде користимо слово A да означимо и матрицу и Абелову групу, али тешко да може да буде неке конфузије!)

У линеарној алгебри користили смо елементарне врста (колона) трансформације. Имали смо трансформације два типа. Први тип је трансформација која се састоји од множења неке врсте (колоне) дате матрице неким инвертибилним скаларом (ознака $V_r := \alpha V_r$ ($K_r := \alpha K_r$) означава да r-ту врсту (колону) множимо скаларом α). Други тип је трансформација која некој врсти (колони) додаје другу врсту (колону) помножену неким скаларом (ознака: $V_r := V_r + \alpha V_r$ за врсте, односно $K_r := K_r + \alpha K_s$ за колоне, где је обавезно $r \neq s$). У случају када радимо, као што је сада, са целобројним матрицама, онда је у првом типу допуштено множење само са 1 и -1 (пошто су то једини цели бројеви који имају инверз у односу на множење), док је у другом случају исто као и код векторских простора (имајући наравно у виду да су бројеви којима множимо цели бројеви). Уз ове елементарне

трансформације, може се додати и трансформација која пермутује две врсте (колоне), а која се може извести композицијом претходно наведених (ово је вероватно прави тренутак да потражите неки уџбеник или свеску из Линеарне алгебре).

Ове операције се могу извести и множењем дате матрице елементарним матрицама (подсетите се овога) и то множењем слева ако „баратамо" са врстама, односно здесна, ако радимо са колонама. Све елементарне матрице су инвертибилне у прстену $M_s(\mathbb{Z})$ (матрица $A \in M_s(\mathbb{Z})$ је инвертибилна у $M_s(\mathbb{Z})$ уколико постоји матрица $B \in M_s(\mathbb{Z})$ за коју је $A \cdot B = I_s$, где је са I_s означена јединична матрица реда s; квадратна матрица из $M_s(\mathbb{Z})$ је инвертибилна акко јој је детерминанта једнака 1 или -1). Наводимо сада, без доказа, теорему која утврђује да постоје тражене трансформације (њен доказ није тежи од доказа да је свака коначно генерисана Абелова група изоморфна директном производу цикличних, али резултат који даје је заправо то, а тако нешто смо већ доказали, па нема потребе да изводимо и овај доказ – вероватно читаоцима неће превише недостајати још један доказ ☺).

Теорема 111 Нека је $A \in M_{mn}(\mathbb{Z})$. Тада постоје инвертибилне матрице $P \in \mathbb{M}_m(\mathbb{Z})$ и $Q \in \mathbb{M}_n(\mathbb{Z})$ тако да је $PAQ = A^0$, при чему је

$$A^0 = \left[\begin{array}{cccc|c} d_1 & 0 & \cdots & 0 & \\ 0 & d_2 & \cdots & 0 & \\ \vdots & \ddots & & \vdots & \mathbf{0} \\ 0 & 0 & \cdots & d_k & \\ \hline \multicolumn{4}{c|}{\mathbf{0}} & \mathbf{0} \end{array}\right]$$

и $d_i \mid d_{i+1}$ за $i = \overline{1, k-1}$. □

Како је множење инвертибилним матрицама еквивалентно вишеструкој примени елементарних трансформација, то закључујемо да њиховом применом можемо добити матрицу траженог облика, односно релације међу почетним генераторима свести на једноставне релације међу (највероватније) неким другим генераторима.

Множење елементарним матрицама слева одговара елементарним трансформацијама на врстама, док множење здесна одговара трансформацијама на колонама. Трансформације врста мењају релације међу генераторима, али не и саме генераторе, док трансформације на колонама мењају генераторе.

Нека су генератори $x_1, \ldots, x_n$ и релације међу генераторима задате матрицом A, тј. релације су задате са

$$AX = \mathbf{0}.$$

Уколико је $PAQ = A^0$, онда множењем горње релације матрицом P слева добијамо

$$PAX = \mathbf{0}.$$

Сада, уметањем производа $Q \cdot Q^{-1}$ добијамо

$$(PAQ)(Q^{-1}X) = \mathbf{0}.$$

Стога, ако са $Y = Q^{-1}X$ означимо нови систем генератора, добијамо

$$A^0 Y = \mathbf{0}.$$

Покажимо како ово у пракси можемо извести, тј. како да погодно региструјемо и нове релације и нове генераторе. Формирајмо матрицу

$$R = \left[\begin{array}{c|c} A & \mathbf{0} \\ \hline & x_1 \\ I_n & \vdots \\ & x_n \end{array}\right].$$

Циљ је на позицији матрице A добити матрицу A^0 трансформацијом врста и колона. Наравно у току рада изводићемо и трансформације врста и колона у произвољном поретку, али да бисмо појаснили шта се дешава, можемо претпоставити да смо прво извели све потребне трансформације на врстама, а потом на колонама. Трансформације на врстама (и то наравно само на првих m врста „велике" матрице, пошто желимо матрицу A да доведемо на тражен облик) доводе до еквивалентне матрице

$$R_1 = \left[\begin{array}{c|c} PA & \mathbf{0} \\ \hline & x_1 \\ I_n & \vdots \\ & x_n \end{array}\right].$$

Сада вршимо трансформацију на колонама да бисмо добили матрицу A^0, али тиме мењамо и колоне у јединичној матрици. Тако добијамо нову матрицу

$$R_2 = \left[\begin{array}{c|c} PAQ & \mathbf{0} \\ \hline & x_1 \\ Q & \vdots \\ & x_n \end{array}\right].$$

Сада желимо да поново добијемо јединичну матрицу уместо матрице Q, тј. да идентификујемо нове генераторе и то изводимо трансформацијом на врстама, али само на „доњим" врстама. Тако напокон добијамо матрицу

$$R = \left[\begin{array}{c|c} A^0 & \mathbf{0} \\ \hline & y_1 \\ I_n & \vdots \\ & y_n \end{array}\right],$$

где је $A^0 = PAQ$, а $Y = Q^{-1}X$ (I_n добијамо множењем слева матрицом Q^{-1}).

Урадимо пар примера.

Пример 112 Нека је Абелова група A задата генераторима x_1, x_2, x_3 и релацијама

$$\begin{aligned} 2x_1 - 4x_2 + 2x_3 &= 0 \\ 4x_1 + 4x_2 - 8x_3 &= 0. \end{aligned}$$

Одредити нормалну форму ове групе.

Решење. Полазимо од матрице

$$R = \left[\begin{array}{ccc|c} 2 & -4 & 2 & 0 \\ 4 & 4 & -8 & 0 \\ \hline 1 & 0 & 0 & x_1 \\ 0 & 1 & 0 & x_2 \\ 0 & 0 & 1 & x_3 \end{array}\right]$$

Трансформацијом $V_2 := V_2 - 2V_1$, добијамо матрицу

$$R_1 = \left[\begin{array}{ccc|c} 2 & -4 & 2 & 0 \\ 0 & 12 & -12 & 0 \\ \hline 1 & 0 & 0 & x_1 \\ 0 & 1 & 0 & x_2 \\ 0 & 0 & 1 & x_3 \end{array}\right]$$

Трансформацијама $K_2 := K_2 + 2K_1$ и $K_3 := K_3 - K_1$, добијамо

$$R_2 = \left[\begin{array}{ccc|c} 2 & 0 & 0 & 0 \\ 0 & 12 & -12 & 0 \\ \hline 1 & 2 & -1 & x_1 \\ 0 & 1 & 0 & x_2 \\ 0 & 0 & 1 & x_3 \end{array}\right]$$

Трансформација $K_3 := K_3 + K_2$ доводи до матрице

$$R_3 = \left[\begin{array}{ccc|c} 2 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 \\ \hline 1 & 2 & 1 & x_1 \\ 0 & 1 & 1 & x_2 \\ 0 & 0 & 1 & x_3 \end{array}\right]$$

С обзиром да $2 \mid 12$, добили смо тражену матрицу A^0. Преостаје да идентификујемо генераторе. Трансформације $V_3 := V_3 - V_5$ и $V_4 := V_4 - V_5$ дају матрицу

$$R_4 = \left[\begin{array}{ccc|c} 2 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 \\ \hline 1 & 2 & 0 & x_1 - x_3 \\ 0 & 1 & 0 & x_2 - x_3 \\ 0 & 0 & 1 & x_3 \end{array}\right]$$

Најзад, трансформација $V_3 := V_3 - 2V_4$ доводи до матрице

$$R_5 = \left[\begin{array}{ccc|l} 2 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 \\ \hline 1 & 0 & 0 & x_1 - 2x_2 + x_3 \\ 0 & 1 & 0 & x_2 - x_3 \\ 0 & 0 & 1 & x_3 \end{array}\right]$$

Дакле, нови генератори су $y_1 = x_1 - 2x_2 + x_3$, $y_2 = x_2 - x_3$ и $y_3 = x_3$, а релације међу њима су $2y_1 = 0$, $12y_2 = 0$. Закључујемо да је нормална форма дате групе: $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}$. ♣

Пример 113 Група је задата генераторима x_1, x_2, x_3, x_4 и релацијама

$$\begin{aligned} 5x_1 + 3x_2 - 3x_4 &= 0 \\ 2x_1 + 4x_2 - 2x_3 &= 0 \\ 7x_1 + 7x_2 - 2x_3 - 3x_4 &= 0. \end{aligned}$$

Одредити њену нормалну форму.

Решење. Полазимо од матрице (обратите пажњу да ли неки генератор учествује у датој релацији!).

$$R = \left[\begin{array}{cccc|l} 5 & 3 & 0 & -3 & 0 \\ 2 & 4 & -2 & 0 & 0 \\ 7 & 7 & -2 & -3 & 0 \\ \hline 1 & 0 & 0 & 0 & x_1 \\ 0 & 1 & 0 & 0 & x_2 \\ 0 & 0 & 1 & 0 & x_3 \\ 0 & 0 & 0 & 1 & x_4 \end{array}\right]$$

Увек је корисно одредити највећи заједнички делилац свих компонената матрице A. Тај број ће заправо бити тражени d_1. Њега треба поставити на позицију $(1,1)$ и онда га искористити да се „почисте" елементи прве врсте и прве колоне. После тога се прелази на подматрицу која има једну врсту и једну колону мање и поступак се наставља.

У нашем случају лако је уверити се да је тај највећи заједнички делилац једнак 1. Трансформацијом $V_1 := V_1 - 2V_2$, добијамо матрицу

$$R_1 = \left[\begin{array}{cccc|l} 1 & -5 & 4 & -3 & 0 \\ 2 & 4 & -2 & 0 & 0 \\ 7 & 7 & -2 & -3 & 0 \\ \hline 1 & 0 & 0 & 0 & x_1 \\ 0 & 1 & 0 & 0 & x_2 \\ 0 & 0 & 1 & 0 & x_3 \\ 0 & 0 & 0 & 1 & x_4 \end{array}\right].$$

Трансформације $V_2 := V_2 - 2V_1$ и $V_3 := V_3 - 7V_1$ дају матрицу

$$R_2 = \left[\begin{array}{cccc|c} 1 & -5 & 4 & -3 & 0 \\ 0 & 14 & -10 & 6 & 0 \\ 0 & 42 & -30 & 18 & 0 \\ \hline 1 & 0 & 0 & 0 & x_1 \\ 0 & 1 & 0 & 0 & x_2 \\ 0 & 0 & 1 & 0 & x_3 \\ 0 & 0 & 0 & 1 & x_4 \end{array}\right].$$

Трансформације $K_2 := K_2 + 5K_1$, $K_3 := K_3 - 4K_1$ и $K_4 = K_4 + 3K_1$ дају матрицу

$$R_3 = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 14 & -10 & 6 & 0 \\ 0 & 42 & -30 & 18 & 0 \\ \hline 1 & 5 & -4 & 3 & x_1 \\ 0 & 1 & 0 & 0 & x_2 \\ 0 & 0 & 1 & 0 & x_3 \\ 0 & 0 & 0 & 1 & x_4 \end{array}\right].$$

Сада се можемо концентрисати на матрицу

$$\left[\begin{array}{ccc} 14 & -10 & 6 \\ 42 & -30 & 18 \end{array}\right].$$

Јасно је да је овде највећи заједнички делилац 2. После трансформације $K_2 := K_2 - 2K_4$ добијамо матрицу

$$R_4 = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & -10 & 6 & 0 \\ 0 & 6 & -30 & 18 & 0 \\ \hline 1 & -1 & -4 & 3 & x_1 \\ 0 & 1 & 0 & 0 & x_2 \\ 0 & 0 & 1 & 0 & x_3 \\ 0 & -2 & 0 & 1 & x_4 \end{array}\right].$$

Применимо трансформацију $V_3 := V_3 - 3V_2$. Добијамо

$$R_5 = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & -10 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \hline 1 & -1 & -4 & 3 & x_1 \\ 0 & 1 & 0 & 0 & x_2 \\ 0 & 0 & 1 & 0 & x_3 \\ 0 & -2 & 0 & 1 & x_4 \end{array}\right].$$

Трансформације $K_3 := K_3 + 5K_2$ и $K_4 := K_4 - 3K_2$ завршавају први део

(одређивање матрице A^0):

$$R_6 = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \hline 1 & -1 & -9 & 6 & x_1 \\ 0 & 1 & 5 & -3 & x_2 \\ 0 & 0 & 1 & 0 & x_3 \\ 0 & -2 & -10 & 7 & x_4 \end{array}\right].$$

Трансформације $V_4 := V_4 + V_5$ и $V_7 := V_7 + 2V_5$ дају

$$R_7 = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & -4 & 3 & x_1 + x_2 \\ 0 & 1 & 5 & -3 & x_2 \\ 0 & 0 & 1 & 0 & x_3 \\ 0 & 0 & 0 & 1 & 2x_2 + x_4 \end{array}\right].$$

После трансформација $V_4 := V_4 - 3V_7$ и $V_5 := V_5 + 3V_7$, добијамо

$$R_8 = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & -4 & 0 & x_1 - 5x_2 - 3x_4 \\ 0 & 1 & 5 & 0 & 7x_2 + 3x_4 \\ 0 & 0 & 1 & 0 & x_3 \\ 0 & 0 & 0 & 1 & 2x_2 + x_4 \end{array}\right].$$

Завршавамо наш рад применом трансформација $V_4 := V_4 + 4V_6$ и $V_5 := V_5 - 5V_6$:

$$R_9 = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & x_1 - 5x_2 + 4x_3 - 3x_4 \\ 0 & 1 & 0 & 0 & 7x_2 - 5x_3 + 3x_4 \\ 0 & 0 & 1 & 0 & x_3 \\ 0 & 0 & 0 & 1 & 2x_2 + x_4 \end{array}\right].$$

Дакле, нови генератори су

$$\begin{aligned} y_1 &= x_1 - 5x_2 + 4x_3 - 3x_4 \\ y_2 &= 7x_2 - 5x_3 + 3x_4 \\ y_3 &= x_3 \\ y_4 &= 2x_2 + x_4, \end{aligned}$$

док су релације међу тим генераторима: $y_1 = 0$, $2y_2 = 0$. Видимо да је један генератор сувишан, тј. почетни систем није био минималан систем генератора. Нормална форма дате групе је $\mathbb{Z}_2 \times \mathbb{Z} \times \mathbb{Z}$. ♣

Комутативни прстени са јединицом; поља

Завршни део курса започињемо дефиницијом појма комутативног прстена са јединицом.

Дефиниција 114 Комутативан прстен са јединицом је структура $(A, +, \cdot)$ за коју важи:

1. $(A, +)$ је Абелова група;
2. $(A, \cdot)$ је комутативан моноид;
3. за све $x, y, z \in A$: $x \cdot (y + z) = x \cdot y + x \cdot z$.

Неутрал у односу на сабирање означавамо са 0, или са 0_A уколико је потребно да избегнемо недоумице, док неутрал у односу на множење означавамо са 1, односно 1_A. Неутрал у односу на сабирање зове се нула, а неутрал у односу на множење јединица прстена. Како ћемо се искључиво бавити комутативним прстенима са јединицом, то ћемо, ради краткоће, понекад користити само термин прстем (подразумевајући да се ради о комутативном прстену са јединицом).

Приметимо да је производ ма ког елемента прстена и нуле једнак нули. Наиме, $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Како је прстен Абелова група у односу на сабирање, то елемент $a \cdot 0$ има инверз (у односу на сабирање) и добијамо да је $0 = a \cdot 0$. Поставља се питање: може ли у неком прстену A важити једнакост $0_A = 1_A$? Уколико је то тако и ако је $x \in A$ произвољан елемент, добијамо да је

$$x = x \cdot 1_A = x \cdot 0_A = 0_A.$$

Дакле, у том случају бисмо добили да је $A = \{0_A\}$. Такав прстен називамо и нула прстен. У даљем ћемо претпоставити да прстени са којима радимо нису нула прстени, тј. да је $0 \neq 1$ у прстену.

У произвољном прстену може се десити да је $x \cdot y = 0$, а да је и $x \neq 0$ и $y \neq 0$. На пример, у прстену $\mathbb{Z}_6$ (у коме су операције сабирање по модулу 6 и множење по модулу 6) важи: $2 \cdot 3 = 0$, а $2, 3 \neq 0$. Имамо посебан назив за такве елементе.

Дефиниција 115 Елемент a прстена A је делитељ нуле уколико постоји елемент $b \neq 0$ за који је $a \cdot b = 0$. Уколико је a делитељ нуле и $a \neq 0$, онда је a прави делитељ нуле.

Скуп свих делитеља нуле у прстену A означавамо са $Z(A)$.

Дефиниција 116 Елемент a прстена A је регуларан уколико за све $x, y \in A$ важи: ако је $a \cdot x = a \cdot y$, онда је $x = y$.

Дакле, регуларни су они елементи које можемо да „скратимо". Приметимо да је елемент регуларан ако и само ако он није делитељ нуле. Наиме, претпоставимо да је a регуларан елемент. Уколико би он био делитељ нуле, онда би следило да је $a \cdot b = 0$ за неки $b \neq 0$. Но, из једнакости $a \cdot b = a \cdot 0$ следи да је $b = 0$. С друге стране, ако a није делитељ нуле и ако је $a \cdot x = a \cdot y$, добијамо да је $a \cdot (x - y) = 0$. Из чињенице да a није делитељ нуле, следи да мора бити $x - y = 0$, те закључујемо да је a регуларан елемент.

Скуп свих регуларних елемената прстена A означавамо са $R(A)$. На основу претходне анализе, добијамо да је $A = Z(A) \sqcup R(A)$.

Дефиниција 117 Елемент a прстена A је инвертибилан уколико постоји елемент $b \in A$ за који је $a \cdot b = 1$.

Уколико је a инвертибилан, онда је елемент b за који важи $a \cdot b = 1$ јединствено одређен (зашто?) и означавамо га са a^{-1}. Скуп свих инвертибилних елемената прстена A означавамо са $U(A)$. Јасно је да је $(U(A), \cdot)$ једна Абелова група. Зовемо је мултипликативна група прстена. Приметимо да је $U(A) \subseteq R(A)$. Наиме, ако је $a \in U(A)$ и $a \cdot x = a \cdot y$, онда је $a^{-1} \cdot a \cdot x = a^{-1} \cdot a \cdot y$, па је $1 \cdot x = 1 \cdot y$, те је $x = y$.

У општем случају је $R(A) \neq U(A)$. На пример, $R(\mathbb{Z}) = \mathbb{Z} \setminus \{0\}$, док је $U(\mathbb{Z}) = \{-1, 1\}$. Но, занимљив је следећи став.

Став 118 У коначном прстену сваки регуларан елемент је инвертибилан.

Доказ. Нека је прстен A коначан и $a \in R(A)$. Дефинишимо $L_a \colon A \to A$ са: $L_a(x) := a \cdot x$. Из регуларности елемента a следи да је L_a „1–1". Наиме, ако је $L_a(x) = L_a(y)$, то значи да је $a \cdot x = a \cdot y$, а како је a регуларан, добијамо да је $x = y$. Како је A коначан, из чињенице да је $L_a \colon A \to A$ „1–1" следи да је L_a и „на". Стога постоји $b \in A$ за које је $L_a(b) = 1$, тј. $a \cdot b = 1$, те закључујемо да је a инвертибилан. □

Дефиниција 119 Комутативан прстен са јединицом A је домен, ако он не садржи праве делитеље нуле, тј. ако је $Z(A) = \{0\}$. Комутативан прстен са јединицом A је поље уколико је сваки ненула елемент у A инвертибилан, тј. ако је $U(A) = A \setminus \{0\}$.

Очигледно је да је свако поље и домен, док као последицу претходног става добијамо да је сваки коначан домен и поље. Наравно, у општем случају та два појма се не поклапају. На пример, $\mathbb{Z}$ јесте домен, али није поље. У наредном курсу видећемо како се сваком домену може придружити једно поље, али то остаје за касније.

Приметимо да је $U(\mathbb{Z}_n) = \Phi(n)$ и да је $\mathbb{Z}_n$ поље ако и само ако је n прост број (уверите се да је то заиста тако!).

Пређимо сада на појам потпрстена.

Дефиниција 120 Нека су $(A, +_A, \cdot_A)$ и $(B, +_b, \cdot_B)$ два комутативна прстена са јединицом при чему је $B \subseteq A$. Кажемо да је B потпрстен са јединицом прстена A уколико је B уколико је

1. за све $x, y \in B$: $x +_B y = x +_A y$;
2. за све $x, y \in B$: $x \cdot_B y = x \cdot_A y$;
3. $1_B = 1_A$.

Добро нам је познато (зар не?) да из првог услова следи да је $0_B = 0_A$. Но, морамо додати услов да је $1_B = 1_A$. Наиме, то не следи из претходна два услова, као што следећи пример јасно показује.

Пример 121 Нека је $A = \{(0,0),(0,1),(1,0),(1,1)\}$, $B = \{(0,0),(1,0)\}$, а операције су дефинисане по координатама, користећи сабирање и множење по модулу 2. Прецизније:

$$(a,b) + (c,d) := (a +_2 c, b +_2 d);$$

$$(a,b) \cdot (c,d) := (a \cdot_2 c, b \cdot_2 d);$$

Операције на B су рестрикције операција на A. Тада су и A и B комутативни прстени са јединицом, но, док је $0_A = (0,0) = 0_B$, то је $1_A = (1,1) \neq (1,0) = 1_B$. □

Размотримо сада директан производ прстена.

Дефиниција 122 Нека су $(A_1, +^1, \cdot^1), (A_1, +^2, \cdot^2) \ldots, (A_n, +^n, \cdot^n)$ комутативни прстени са јединицом. На скупу $A = A_1 \times A_2 \times \cdots \times A_n$ дефинишемо структуру $(A, +, \cdot)$ са:

$$\begin{aligned}(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) &:= (x_1 +^1 y_1, x_2 +^2 y_2, \ldots, x_n +^n y_n)\\ (x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n) &:= (x_1 \cdot^1 y_1, x_2 \cdot^2 y_2, \ldots, x_n \cdot^n y_n)\end{aligned}$$

Ова структура јесте комутативан прстен са јединицом и представља директан производ прстена $A_1, \ldots, A_n$. Овде је $0_A = (0_{A_1}, \ldots, 0_{A_n})$ и $1_A = (1_{A_1}, \ldots, 1_{A_n})$. Уколико имамо бар два фактора у производу, у њему увек има правих делитеља нуле: $(0_{A_1}, \ldots, 1_{A_n}) \cdot (1_{A_1}, \ldots, 0_{A_n}) = 0_A$. Како у пољу нема правих делитеља нуле (зашто?) закључујемо да производ бар два комутативна прстена са јединицом (чак и ако су сви фактори поља) не може бити поље.

Следећи став утврђује структуру мултипликативне групе директног производа прстена.

Став 123 Ако је $A = A_1 \times \cdots \times A_n$, онда је $U(A) = U(A_1) \times \cdots \times U(A_n)$.

Доказ. Ово није тешко показати.

$\subseteq$: Нека је $a \in U(A)$. То значи да постоји $b \in A$ такав да је $a \cdot b = 1_A$. Другим речима, ако је $a = (a_1, \ldots, a_n)$, онда постоје $b_i \in A_i$ такви да је

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (1_{A_1}, \ldots, 1_{A_n}).$$

Но, ова једнакост је еквивалентна са: $a_i \cdot^i b_i = 1_{A_i}$ за $i = \overline{1,n}$. То управо значи да $a_i \in U(A_i)$ за $i = \overline{1,n}$, тј. $a \in U(A_1) \times \cdots \times U(A_n)$.

$\supseteq$: Нека $a \in U(A_1) \times \cdots \times U(A_n)$. Дакле, $a = (a_1, \ldots, a_n) \in U(A_1) \times \cdots \times U(A_n)$. Према томе, $a_i \in U(A_i)$ за $i = \overline{1,n}$, па постоје $b_i \in A_i$ такви да је $a_i \cdot^i b_i = 1_{A_i}$, за $i = \overline{1,n}$. Но, одатле следи да за елемент $b - (b_1, \ldots, b_n) \in A$ важи: $a \cdot b = 1_A$, те закључујемо да $a \in U(A)$. □

Став 124 Уколико је $(A, +_A, \cdot_A) \cong (B, +_B, \cdot_B)$, онда је $(U(A), \cdot_A) \cong (U(B), \cdot_B)$.

Доказ. Нека је $f\colon A \to B$ изоморфизам прстена. Доказаћемо да је $f[U(A)] = U(B)$. Одатле следи да рестрикција f на $U(A)$ индукује тражени изоморфизам мултипликативних група датих прстена.

$\subseteq$: Нека је $a \in U(A)$. То значи да постоји $a_1 \in A$ тако да је $a \cdot_A a_1 = 1_A$. Но, тада је $f(a \cdot_A a_1) = f(1_A)$, па је $f(a) \cdot_B f(a_1) = 1_B$. Дакле, $f(a) \in U(B)$.

$\supseteq$: Нека $b \in U(B)$. То значи да постоји $b_1 \in B$ тако да је $b \cdot_B b_1 = 1_B$. Како је f „на", постоје a, a_1 за које је $f(a) = b$ и $f(a_1) = b_1$. Тако добијамо

$$f(1_A) = 1_B = b \cdot_B b_1 = f(a) \cdot_B f(a_1) = f(a \cdot_A a_1).$$

С обзиром на то да је f и „1–1", следи да је $1_A = a \cdot_A a_1$, тј. $a \in U(A)$, па $b \in f[U(A)]$. □

Пређимо на неке конкретне примере прстена. Претходни појмови и резултати даће нам, уз мало рада, неке резултате из елементарне теорије бројева.

Теорема 125 Нека су $m_1, m_2, \ldots, m_n \geq 2$ цели бројеви за које је испуњено: $\mathrm{NZD}(m_i, m_j) = 1$ за $i \neq j$. Тада су прстени $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ и $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ изоморфни.

Доказ. Нека је $m = m_1 m_2 \cdots m_n$. Приметимо да оба прстена имају m елемената. Стога је, за доказ постојања изоморфизма, довољно конструисати једну „1–1" функцију из једног у други, која се слаже са операцијама, јер ће та функција сигурно бити и „на", тј. изоморфизам (то су коначни скупови са истим бројем елемената). Ако са $\rho_k(x)$ означимо остатак при (еуклидском) дељењу x са k, онда је тражена функција $f\colon \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ дефинисана са:

$$f(x) := (\rho_{m_1}(x), \rho_{m_2}(x), \ldots, \rho_{m_n}(x)).$$

Докажимо да је f „1–1". Нека је $f(x) = f(y)$. То значи да за $i = \overline{1,n}$ важи: $\rho_{m_i}(x) = \rho_{m_i}(y)$. Но, ако два броја имају исти остатак при дељењу бројем m_i, онда је њихова разлика дељива са m_i. Дакле, за $i = \overline{1,n}$ важи: $m_i \mid (x - y)$. Како су бројеви m_i узајамно прости, следи да $m \mid (x - y)$. С обзиром да $x, y \in Z_m = \{0, 1, \ldots, m-1\}$, добијамо да је $x - y = 0$, тј. $x = y$.

Докажимо да се f слаже са операцијама, тј. да је за све $x, y \in Z_m$: $f(x +_m y) = f(x) + f(y)$ и $f(x \cdot_m y) = f(x) \cdot f(y)$ (где је са $+$, односно $\cdot$ означена операција у директном производу, за коју знамо како се дефинише). Доказаћемо то за операцију множења, док сличан доказ за сабирање остављамо за вежбу.

Дакле, треба доказати да је $f(x \cdot_m y) = f(x) \cdot f(y)$ за све $x, y \in Z_m$. С обзиром на дефиницију функције f и дефиницију операције $\cdot$, ово се своди на доказ чињенице да је за све $i = \overline{1,n}$ испуњено:

$$\rho_{m_i}(x \cdot_m y) = \rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y).$$

Доказ ћемо извести тако што ћемо показати да су и лева и десна страна ове једнакости заправо остаци при дељењу $x \cdot y$ са m (где је овде $\cdot$ операција множења целих бројева). Наиме, по дефиницији операције $\cdot_m$ имамо да је

$$x \cdot y \equiv x \cdot_m y \,(\mathrm{mod}\ m).$$

Приметимо да важи следеће: ако је $a \equiv b \,(\mathrm{mod}\ m)$ и ако $k \mid m$, онда је и $a \equiv b \,(\mathrm{mod}\ k)$. Наиме, $a \equiv b \,(\mathrm{mod}\ m)$ је еквивалентно са $m \mid (a - b)$. Како $k \mid m$, то следи да је и $k \mid (a - b)$, што је еквивалентно са $a \equiv b \,(\mathrm{mod}\ k)$. Стога, из

$$x \cdot y \equiv x \cdot_m y \,(\mathrm{mod}\ m),$$

следи да за све $i = \overline{1,n}$ важи:

$$x \cdot y \equiv x \cdot_m y \,(\mathrm{mod}\ m_i).$$

С обзиром да је

$$x \equiv \rho_k(x) \,(\mathrm{mod}\ k),$$

добијамо да је

$$x \cdot_m y \equiv \rho_{m_i}(x \cdot_m y) \,(\mathrm{mod}\ m_i),$$

те, напокон, добијамо да је

$$x \cdot y \equiv \rho_{m_i}(x \cdot_m y) \,(\mathrm{mod}\ m_i).$$

С обзиром да је $\rho_{m_i}(x \cdot_m y) \in Z_{m_i}$, следи да је тај број заправо остатак при дељењу $x \cdot y$ са m_i.

Како је $x \equiv \rho_{m_i}(x) \,(\mathrm{mod}\ m_i)$ и $y \equiv \rho_{m_i}(y) \,(\mathrm{mod}\ m_i)$, то је

$$\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \equiv x \cdot_{m_i} y \,(\mathrm{mod}\ m_i).$$

Но,

$$x \cdot_{m_i} y \equiv x \cdot y \,(\mathrm{mod}\ m_i),$$

те је и

$$x \cdot y \equiv \rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \,(\mathrm{mod}\ m_i).$$

С обзиром да $\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \in \{0, \ldots, m_i - 1\}$, следи да је $\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \in \{0, \ldots, m_i - 1\}$ остатак при дељењу $x \cdot y$ са m_i. Закључујемо да мора бити

$$\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) = \rho_{m_i}(x \cdot_m y),$$

јер је и један и други број остатак при дељењу $x \cdot y$ са m_i. □

Последица 126 (Кинеска теорема о остацима) Нека су $m_1, m_2, \ldots, m_n \geq 2$ цели бројеви за које је $\mathrm{NZD}(m_i, m_j) = 1$ за $i \neq j$. Тада за произвољне $x_i \in \mathbb{Z}$, $i = \overline{1,n}$, систем конгруенција

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \\ &\vdots \\ x &\equiv x_n \pmod{m_n} \end{aligned} \tag{14}$$

има јединствено решење по модулу $m_1 m_2 \cdots m_n$.

Доказ. Функција f, дефинисана у претходној теореми, је изоморфизам. Ми ћемо искористити чињеницу да је она „на". Нека су $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. Са r_i означимо остатак при дељењу броја x_i са m_i. Јасно је да тада важи $x_i \equiv r_i \pmod{m_i}$, за $i = \overline{1,n}$. Формирајмо n-торку $(r_1, r_2, \ldots, r_n) \in Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_n}$. Како је f „на", то постоји $x \in Z_m$ (где је $m = m_1 m_2 \cdots m_n$) за које је $f(x) = (r_1, r_2, \ldots, r_n)$. Но, с обзиром на дефиницију f, то заправо значи да је $x \equiv r_i \pmod{m_i}$ за $i = \overline{1,n}$ (уверите се да је то заиста тако!), те је и $x \equiv x_i \pmod{m_i}$ за $i = \overline{1,n}$. Дакле, систем конгруенција има решење. Проверимо и јединственост решења. Нека је $x' \in \mathbb{Z}$ неки други цео број за који је $x' \equiv x_i \pmod{m_i}$ за $i = \overline{1,n}$. Добијамо да је $x \equiv x' \pmod{m_i}$ за $i = \overline{1,n}$. То значи да $m_i \mid (x - x')$ за $i = \overline{1,n}$. Како су m_i узајамно прости то даје: $m \mid (x - x')$, те је решење заиста јединствено по модулу m (јединственост решења следи и из чињенице да је f „1–1" – проверите како следи). □

Последица 127 Ако су $m_1, m_2, \ldots, m_n$ цели бројеви за које је $\mathrm{NZD}(m_i, m_j) = 1$, за $i \neq j$, онда је $\varphi(m_1 m_2 \cdots m_n) = \varphi(m_1)\varphi(m_2) \cdots \varphi(m_n)$.

Доказ. На основу претпоставки из доказане теореме следи да важи изоморфизам прстена $\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$. На основу става **??** и става **??** добијамо да је $U(\mathbb{Z}_m) \cong U(\mathbb{Z}_{m_1}) \times \cdots \times U(Z_{m_n})$. С обзиром да је $U(\mathbb{Z}_k) = \Phi(k)$ и да је $\varphi(k) = |\Phi(k)|$, тражени резултат следи (уверите се у то!). □

Као што знамо, уколико је F поље, онда је $U(F) = F \setminus \{0\}$. Ова група, наравно, може бити и бесконачна (ако је поље F бесконачно). Оно што је занимљиво је да имамо врло једноставан опис за коначне подгрупе групе $U(F)$. Најпре докажимо један помоћни став.

Став 128 Нека је A Абелова група реда m и нека је за сваки позитиван цео број d такав да $d \mid m$ број решења једначине $dx = 0$ у групи A највише d, тј.

$$|\{x \in A : dx = 0\}| \leq d. \qquad (*)$$

Тада је група A циклична.

Доказ. На основу теореме о карактеризацији коначних Абелових група, $A \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k}$ за неко $k \geq 1$, при чему је $d_1 > 1$ и $d_i \mid d_{i+1}$ за $i = \overline{1, k-1}$. Да бисмо доказали да је A циклична довољно је (а и потребно) да докажемо да је $k = 1$. На основу раније леме о броју решења једначине $d_1 x = 0$ у оваквом производу, знамо да је тај број једнак $\mathrm{NZD}(d_1, d_1) \cdot \mathrm{NZD}(d_1, d_2) \cdots \mathrm{NZD}(d_1, d_k) = d_1^k$. Но, на основу услова $(*)$, тај број не сме бити већи од d_1, те мора бити $k = 1$. □

Теорема 129 Нека је F поље и $(A, \cdot)$ коначна подгрупа групе $(U(F), \cdot)$. Тада је A циклична група.

Доказ. Нека је ред групе A једнак m и нека $d \mid m$. Како је група A задата мултипликативно, то ћемо у примени претходног става користити мултипликативан запис. Да бисмо доказали да је A циклична, довољно је да докажемо да је

$$\left|\{a \in A : a^d = 1\}\right| \leq d.$$

Но, свако решење једначине $a^d = 1$ у пољу F је заправо нула полинома $p(X) = X^d - 1 \in F[X]$. Сада можемо искористити добро познату чињеницу да ненула полином са коефицијентима у пољу не може имати више нула него што је његов степен. С обзиром да је степен овог полинома једнак d, важи тражена неједнакост и резултат следи. □

Како је $\mathbb{Z}_p$ поље уколико је p прост број, то је група $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ циклична група реда $p-1$. На основу јединствености (до на изоморфизам) цикличних група датог реда следи да је ова група изоморфна групи $(\mathbb{Z}_{p-1}, +_{p-1})$. Но, занимљиво је (и корисно) експлицитније задати тај изоморфизам. У ту сврху уводимо следећу дефиницију.

Дефиниција 130 Ма који генератор цикличне групе $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ назива се примитивни корен по модулу p.

Читалац се може запитати „примитивни корен из чега?" Заправо је то примитивни корен из јединице (јер у $\mathbb{Z}_p$ важи: $x^p = 1$ за све $x \in Z_p$). Ово је повезано са „обичним" коренима из јединице (у пољу $\mathbb{C}$) – подсетите се примера групе $\mathbb{C}_n$ са почетка курса!

Став 131 Нека је p прост број и r ма који примитиван корен из јединице по модулу p. Тада је са:

$$\mathrm{ind}_r(a) = x \text{ **акко** } r^x = a,$$

дефинисан један изоморфизам $\mathrm{ind}_r \colon (\mathbb{Z}_p \setminus \{0\}, \cdot_p) \to (\mathbb{Z}_{p-1}, +_{p-1})$.

(Тешко је не приметити сличност са дефиницијом логаритма за основу r, зар не?)

Доказ. Како је $\mathbb{Z}_p \setminus \{0\} = \langle r \rangle = \{r^0, r^1, \ldots, r^{p-2}\}$, то је јасно да је ind_r једна бијекција. Треба показати да се слаже са операцијама, тј. да је

$$\mathrm{ind}_r(a \cdot_p b) = \mathrm{ind}_r +_{p-1} \mathrm{ind}_r(b),$$

за све $a, b \in Z_p$. У ту сврху, нека је $\mathrm{ind}_r(a) = x$ и $\mathrm{ind}_r(b) = y$. То значи да је $r^x = a$ и $r^y = b$. Дакле,

$$a \cdot_p b = r^x \cdot_p r^y = r^{x+y}.$$

С обзиром да је $r^{p-1} = 1$ у групи $\mathbb{Z}_p$, то је и

$$r^{x+y} = r^{x+_{p-1}y}$$

($x + y$ и $x +_{p-1} y$ разликују за умножак броја $p - 1$). Стога је

$$a \cdot_p b = r^{x+_{p-1}y}.$$

На основу дефиниције ind_r, добијамо да је $x +_{p-1} y = \mathrm{ind}_r(a \cdot_p b)$. Ако се подсетимо шта су x и y, добијамо да је заиста $\mathrm{ind}_r(a) +_{p-1} \mathrm{ind}_r(b) = \mathrm{ind}_r(a \cdot_p b)$, што се и тражило. □

Погледајмо један пример примене примивних корена.

Пример 132 а) Наћи све примитивне корене по модулу 13.
б) Решити конгруенцију $x^5 \equiv 7 \pmod{13}$.

Решење. а) Метод је једноставан. Директном провером нађимо један примитивни корен. Нека је то r. Тада су сви остали примитивни корени једнаки r^x, где је x узајамно прост са 12 (мултипликативна група је реда 12, њен генератор је r – подсетите се реда елемента r^x).

У овом случају, директном провером добијамо да је један примитивни корен једнак 2 (рачунамо у $\mathbb{Z}_{13}$):

$$\begin{aligned}
2^1 &= 2 \\
2^2 &= 4 \\
2^3 &= 8 \\
2^4 &= 3 \\
2^5 &= 6 \\
2^6 &= 12 \\
2^7 &= 11 \\
2^8 &= 5 \\
2^{10} &= 10 \\
2^{11} &= 7 \\
2^{12} &= 1.
\end{aligned}$$

Дакле, примитивни корени су још и $2^5 = 6$, $2^7 = 11$ и $2^{11} = 7$. Због примене на решавање конгруенција, погодно је направити и следећу табелу.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_r(a)$	0	1	4	2	9	5	11	3	8	10	7	6

б) Нека је $\overline{x}$ остатак при дељењу x са 13 и $y = \mathrm{ind}_2(\overline{x})$. Тада се

$$x^5 \equiv 7 \,(\mathrm{mod}\ 13)$$

своди на

$$5y \equiv \mathrm{ind}_2(7) \,(\mathrm{mod}\ 12),$$

$(x^5 \equiv \overline{x}^5 \,(\mathrm{mod}\ 13))$, тј. на

$$5y \equiv 11 \,(\mathrm{mod}\ 12).$$

С обзиром да је $5 \cdot 5 \equiv 1 \,(\mathrm{mod}\ 12)$ и да је $55 \equiv 7 \,(\mathrm{mod}\ 12)$, добијамо да је $y = 7$ $(y \in \mathbb{Z}_{12})$. С обзиром да из $\mathrm{ind}_2(\overline{x}) = 7$ следи да је $\overline{x} = 11$ (погледајте таблицу), добијамо и тражено решење: $x \equiv 11 \,(\mathrm{mod}\ 13)$ ♣

За сам крај курса оставили смо једну познату теорему из елементарне теорије бројева.

Теорема 133 *(*Вилсонова теорема*)* Нека је p прост број. Тада је

$$(p-1)! \equiv -1 \,(\mathrm{mod}\ p).$$

Доказ. Ако је $p = 2$, све је јасно. Претпоставимо да је p непаран прост број. Уочимо полином $q(X) = X^{p-1} - 1 \in \mathbb{Z}_p[X]$. То је полином степена $p-1$ и у пољу он може имати највише $p-1$ различиту нулу. С обзиром да је за све $a \in \{1, \ldots, p-1\}$: $a^{p-1} \equiv 1 \,(\mathrm{mod}\ p)$, то су све нуле полинома $q(X)$ заправо $1, 2, \ldots, p-1$ (из поља $\mathbb{Z}_p$). Стога је

$$q(X) = (X-1)(X-2)\cdots(X-(p-1)).$$

Добијамо да је

$$q(0) = (0-1)(0-2)\cdots(0-(p-1)),$$

односно

$$-1 = (-1)(-2)\cdots(-(p-1)),$$

у пољу $\mathbb{Z}_p$. Преласком на целе бројеве добијамо да је

$$-1 \equiv (-1)(-2)\cdots(-(p-1)) \,(\mathrm{mod}\ p),$$

тј.

$$-1 \equiv (-1)^{p-1} 1 \cdot 2 \cdots (p-1) \,(\mathrm{mod}\ p),$$

С обзиром да је p непаран, добијамо да је

$$-1 \equiv (p-1)! \,(\mathrm{mod}\ p),$$

што је и тражено. □